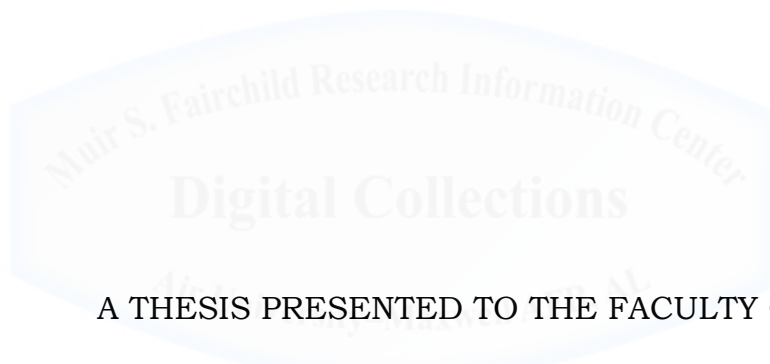


A GREY AREA:  
CONGRESSIONAL OVERSIGHT OF THE MIDDLE GROUND BETWEEN  
TITLE 10 AND TITLE 50

BY

MICHAEL D. CURRY, Lieutenant Colonel, USAF



A THESIS PRESENTED TO THE FACULTY OF  
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES  
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2012

**APPROVAL**

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

---

Dr. JAMES D. KIRAS

---

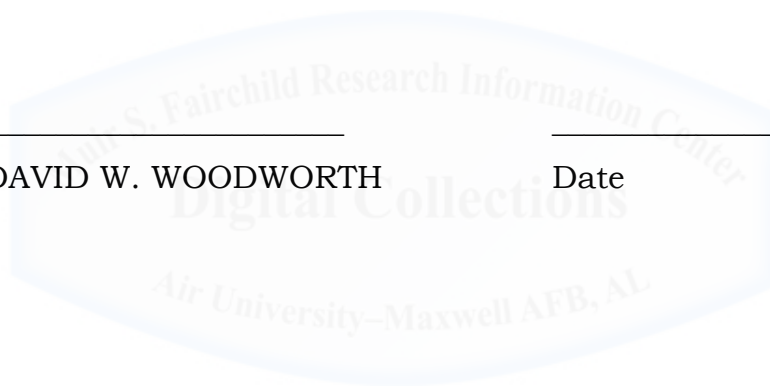
Date

---

Lt Col DAVID W. WOODWORTH

---

Date



**DISCLAIMER**

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.



## **ABOUT THE AUTHOR**

Lieutenant Colonel Michael D. Curry received his commission from the United States Air Force Academy in 1998. While awaiting pilot training he served as wing scheduler with the 4<sup>th</sup> Fighter Wing at Seymour Johnson Air Force Base in North Carolina. He attended undergraduate pilot training at Laughlin Air Force Base and Naval Air Station Corpus Christi, both in Texas. After receiving his wings he transitioned to the 8th Special Operations Squadron at Duke Field, Florida, where he flew the mighty Combat Talon I. After spending five years and countless deployments with the 8th he transitioned to another Air Force Special Operations Command Squadron employed at all levels of warfare. Prior to attending for school he served fourteen months as the Aide to Secretary of the Air Force Michael B. Donley.

Lieutenant Colonel Curry has a bachelor's degree in General Engineering from the United States Air Force Academy and a Master's Degree in Aerospace Science with Specialization in Operations from Embry-Riddle Aeronautical University. In 2011 he received a Master's in Public Administration from Harvard's John F. Kennedy School of Government. Following graduation from the School of Advanced Air and Space Studies he will return to a Special Operations Squadron as the Director of Operations.

## **ACKNOWLEDGMENTS**

I would like to thank Dr. James Kiras for his mentorship over this year without which would have made my tortured writing of this thesis even worse. In addition, Lt Col David Woodworth provided a highly useful review of the thesis and saved me from more than a few embarrassments on the page.

Most of all I would like to thank my family for enduring all the moves over the last few years culminating in our move to SAASS. This year has not been easy on anyone and they have borne the brunt for sure. Without this experience there is no way my three and five year olds would be walking around coloring in coloring books comparing how many pages they completed in their “thesis” with how many Daddy had done. (They always seemed to be ahead of me!)



## **ABSTRACT**

This thesis examines the divide between Title 10 and Title 50 from a congressional oversight perspective. Beginning by explaining the origins of modern intelligence committee oversight and the legal framework supporting it the author sets up two case study relationships. The first case study explores the complex relationship between the military's Special Operations Command the Central Intelligence Agency. The second surveys the developing relationship between the National Security Agency and Cyber Command. After breaking down these interactions in detail the final chapter considers changes in the contemporary strategic environment and identifies challenges threats today, and our responses to them, pose to oversight. Finally the author recommends changes to oversight to ensure that operations that straddle the Title 10/50 divide are reviewed, authorized, and executed appropriately.



## CONTENTS

Chapter	Page
DISCLAIMER.....	ii
ABOUT THE AUTHOR .....	iii
ACKNOWLEDGMENTS .....	iv
ABSTRACT .....	v
INTRODUCTION .....	1
1 YESTERDAY AND TODAY .....	9
2 SOCOM AND THE CIA .....	28
3 CYBERCOM AND THE NSA: TWO BODIES, ONE HEAD .....	44
4 POLICY CONSIDERATIONS SINCE 9/11 .....	59
CONCLUSION .....	74
ACRONYMS .....	83
BIBLIOGRAPHY .....	84

## Illustrations

### Table

1	Characteristics .....	23
2	Characteristics (CIA & SOCOM) .....	33
3	Characteristics (Cyber) .....	48
4	Proposed Select Intelligence Committee Structure .....	80

## INTRODUCTION

*If oversight is to function better, you first need it to function [at all].*

Former Senate Select Committee on Intelligence Chairman Birch Bayh

On December 22, 1974, Seymour Hersh drastically influenced the relationship between Congress and the intelligence community. In his front page article for the *New York Times*, Hersh exposed the Central Intelligence Agency's (CIA) "family jewels." These jewels comprised a collection of agency covert actions dating back to the 1950's, just a few short years after the Agency's creation.<sup>1</sup> With Watergate fresh on the country's mind having just witnessed President Nixon's resignation only five months earlier, Washington was abuzz with questions about how the CIA, trusted with so much, could stray so far. President Ford established the Rockefeller Commission, the Senate the Church Committee, and the House of Representatives the Pike Commission all within six months of Hersh's article.<sup>2</sup> The immediate reaction by Congress to the news was swift. Long before any of the commissions reported out, Congress enacted the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961. This amendment constrained the independent actions of the CIA and forced the President to disclose all covert actions to Congress.<sup>3</sup> Hersh's disclosures, which brought scrutiny of covert action excesses, are one of a number of examples where public exposure resulted in more strict legislation.

---

<sup>1</sup> Seymour M. Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times*, 22 December 1974, A1.

<sup>2</sup> Executive Order 11828, Establishing a Commission on CIA Activities Within the United States, 4 January 1975. *Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, SR 21, 94th Cong., 1st sess., 27 January 1975. And *House Select Committee on Intelligence*. HR 138, 94th Cong., 1st sess., 19 February 1975.

<sup>3</sup> *Foreign Assistance Act of 1961*, Public Law 93-559, 93rd Cong., 2nd sess. (30 December 1974), sec 662.

Congressional oversight of the executive branch of the United States Government is one part of the system of checks and balances built by the framers into the United States Constitution between the three branches of government. This oversight needs to strike a delicate balance between control and execution authority, in order to not unduly hamper operations and effectiveness and elevate the responsibility for oversight over the Agency to the people's elected representatives of the United States. In the past, significant departmental failure or overreach drove the need for additional congressional oversight, and this oversight sometimes occurred at a painful operational or organizational price. This thesis examines Congressional oversight over the intelligence community, the military and the sometimes blurry lines that occur in interagency cooperation between the two. At first glance it appears that appropriate oversight is already enshrined legally. US law, for example, codifies roles and responsibilities for the military under Title 10 United States Code (U.S. Code), Armed Forces.<sup>4</sup> In contrast Title 50 USC, War and National Defense, deals mainly with the definitions and activities of the intelligence community.<sup>5</sup> These stovepipes for authorities and oversight, designed for an earlier time, struggle to deal with the complex challenges of present day. The security environment facing the country now requires the most prepared, best postured agency deal with each situation as it arises regardless of what Congressional committee they report to. When the President directs an activity that does not fall neatly within the titles nestled in the US Code how does Congress maintain their ability to provide oversight?

Representatives within Congress as well as those within the Executive Branch became aware of such gaps and overlaps when terrorists exploited them to attack the United States on September 11, 2001. To address such overlaps, President George Bush formed a

---

<sup>4</sup> 10 U.S.C. (1956)

<sup>5</sup> 50 U.S.C. (1917)

commission to investigate the attacks. The National Commission on Terrorist Attacks Upon the United States, better known as the 9/11 Commission, reviewed 2.5 million pages, interviewed more than 1,200 individuals, and held 19 days of hearings to identify gaps and overlaps and recommend changes to statutes and authorities.<sup>6</sup> One of the Commission's specific recommendations related to the overlap between Title 10 and 50 authorities was that US Special Operations Command should be lead agency for all clandestine and covert paramilitary operations.<sup>7</sup> This recommendation strove to "concentrate responsibility and necessary legal authorities in one entity."<sup>8</sup> Despite the apparent common sense of the recommendation, and a number of studies involving key department and agency stakeholders, the divide between Titles 10 and 50 authorities with all of their inherent ambiguity remains in place.

The arguments inherent in the two Titles have been subject of study in professional military education and elsewhere. In 2003 Colonel Kathryn Stone, a practicing US Army lawyer, studied this vexing problem primarily from the perspective of the clandestine authorities of the CIA to conduct Title 10 military operations in Afghanistan and, in particular, she focused specifically on the legal issues.<sup>9</sup> The legal argument the Agency faces while conducting military operations is identical to the one military operators confront when they operate on covert authorities. Stone's critical analysis focused on the law as it pertains in a state of war but she did not expound on the difficulties experienced by the same

---

<sup>6</sup> National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States*. (New York: W. W. Norton & Company, 2004), xv.

<sup>7</sup> National Commission on Terrorist Attacks, 415.

<sup>8</sup> National Commission on Terrorist Attacks, 415.

<sup>9</sup> COL Kathryn Stone, *All Necessary Means—Employing CIA Operatives in a Warfighting Role Alongside Special Operations Forces*, (Carlisle Barracks, PA: U.S. Army War College, 2003), iii.

interagency team when in a state of peace.<sup>10</sup> Colonel Richard Gross (US Army) examined the same problem but from the perspective of the military authorities required for Special Operations Forces (SOF) to conduct covert action as opposed to clandestine operations in a 2009 Army War College monograph.<sup>11</sup> His work concentrated on examined covert action and clandestine activities from a command perspective using it as the main way to differentiate between authorities granted within the legislated framework of Title 10 and Title 50.<sup>12</sup> In the discourse surrounding Titles 10 and 50 both works have merit. However, they only scratch the surface of the issues swirling this debate. Both authors accurately describe the complexities involved from their vantage point but delve into the details so quickly they gloss over potential solutions.<sup>13</sup>

### Definitions

Much confusion exists between Title 10 and Title 50 operations over the following terms: covert (and in particular, “covert action”), clandestine, and traditional military activity. Some of the definitions are present in the Code itself while others lack specific legal definition and department-specific publications or guidance offer the only explanation.

Covert action is defined by Title 50 USC as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly.”<sup>14</sup> Title 50 also establishes the CIA as the lead agency in most

---

<sup>10</sup> Stone. Colonel Stone identifies Congressional Oversight as one area for further study during her research but does not look at this issue in depth.

<sup>11</sup> Col Richard Gross, *Different Worlds: Unacknowledged Special Operations and Covert Action*, (Carlisle Barracks, PA: U.S. Army War College, 2009), ABSTRACT.

<sup>12</sup> Gross, 2.

<sup>13</sup> In addition to Stone and Gross the following authors also discuss challenges in this field. Alfred Cumming authored several Congressional Research Service reports. Andru E. Wall wrote in the Harvard National Security Journal. Robert Chesney wrote on the subject in the Journal of National Security Law and Policy. Finally, Paul A. Walker wrote about Traditional Military Activity and Cyber.

<sup>14</sup> 50 U.S.C. § 413b (e)

covert actions while providing for other organizations or departments to participate under CIA rules or rules specifically developed for covert action.<sup>15</sup>

There are some exemptions provided to exclusive CIA responsibility for covert action specifically where the military is concerned. This is the initial source of much of the confusion between Title 10 and Title 50 activities. Nothing bars the Department of Defense from covert action *per se*. Title 50 allows the military to conduct the following covert activities: those whose primary purpose is acquiring intelligence, counterintelligence, traditional activities for operational security of government programs, routine support to overt activities, and traditional military activity.<sup>16</sup>

Unlike the clear definition of “covert action,” U.S. Code does not provide similar clarity or legal precision for the term “clandestine.” One must search Department of Defense (DoD) publications, such as joint doctrine, for a definition of what is considered clandestine. For example, Joint publication 3.05 defines a clandestine operation as “an operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment.”<sup>17</sup> The major operational difference between a covert action and a clandestine one is the concealment of only the operation and not the agency who conducted it.<sup>18</sup>

The last term that leads to confusion is “traditional military activity,” or TMA. One problem with TMA is the difficulty in finding specific definitions and even those have changed over time. Buried in the House of Representatives Report accompanying the Intelligence Authorization Act of 1991 is one of the most explicit definitions of TMA.

---

<sup>15</sup> 50 U.S.C. § 413b(a(3))

<sup>16</sup> 50 U.S.C. § 413b (e)

<sup>17</sup> Joint Publication 3-05.1 *Joint Special Operations Task Force Operations*, 26 April 2007 GL-10

<sup>18</sup> Joint Pub 3-05.1 *Joint Special Operations Task Force Operations*, GL-10.

In this report the conferees defined TMA to include activities while under the “direction and control” of a US military commander in direct support of ongoing or anticipated hostilities where the role of the government will be publicly acknowledged.<sup>19</sup> This definition allows for a clear break between itself and the one for covert action. The subtleties within the definitions are the frontlines for the debates about Titles 10 and 50.

Even a cursory comparison of these terms shows that the lines of authority and agency between them are thin and blurry. Given the unclear lines of delineation between covert and clandestine action, as well as TMA, those within departments, agencies, and elsewhere are left to interpret whether or not their actions are crossing lines of authority. When coupled with existing mechanisms for congressional oversight it is easy to see how operating between these distinct U.S. Code titles can be exceptionally confusing to those charged with operating under and between them.

### **Methodology**

Where previous studies have examined the legal definitions as the answer to problems dealing with Title 10 and Title 50 this study will look specifically at congressional oversight of the existing legislative framework. The gray area between them existed prior to 9/11 but subsequently there has been a marked increase in interagency cooperation to make operations more effective. In addition, since 9/11 cyberspace is an emerging and increasingly dominant domain. The executive branch of government spread specific capabilities and authorities required to operate offensively and defensively bringing confusion over the dividing line between Title 10 and Title 50 authorities into relief. The problems related to who is authorized to do what, and

---

<sup>19</sup> House, *Joint Explanatory Statement of the Committee of Conference*, 102nd Cong., 1st sess., 1991, HR 1455.

who and under what conditions should provide oversight of Title 10 and Title 50 activities is one that will not going away any time soon.

In Chapter One this thesis examines the origins of contemporary oversight and in particular, how and why current oversight of the intelligence community has evolved. It further examines why the Title 10 and 50 stovepipes evolved like they did and with this foundation in place, the chapter compares and contrasts specific characteristics of covert, clandestine, and traditional military activities.

Chapter Two explores how the Title 10 and Title 50 divide affects two of the primary organizations involved in covert and clandestine operations, the United States Special Operations Command (SOCOM) and the CIA. The chapter looks specifically at the recommendations of the 9/11 Commission as a means to explore the issues of capability creep and overlap between them. The chapter concludes with an examination of the current authorities Congress has granted both organizations and how they interact with each other before deciphering if this relationship is sustainable.

Chapter Three shines light on the emerging cyber domain paying particular attention to how CYBERCOM and the National Security Agency deal with problems of authority and oversight. The chapter moves on to analysis of intelligence gathering versus operational preparation of the environment to illuminate how these seemingly similar functions are separate. Finally the chapter looks at the command issues related to cyberspace and in particular, the implications of uniformed military members in leadership roles in both a civilian agency and a military one.

Chapter Four focuses on the Title 10 Title 50 divide since 9/11. It examines the new strategic environment facing policy makers today and analyzes how congressional oversight has kept pace with this environment. Then it moves onto the three most significant reasons the

Title 10/50 problem continues: declining budget authority; increased use of interagency solutions; and, Congressional misalignment with the current threat that prevents effective oversight from occurring.

Congressional oversight is not a tax on capability. Oversight is there to protect the operators, executive branch policy makers, and legislators. Ignoring the problems present in the current system will not make them go away. One can either take a proactive stance to remedy the problem or wait for the next front page story to cause a wild pendulum swing.



## **CHAPTER 1**

### **YESTERDAY AND TODAY**

*There are things that my government does that I would rather not know about.*

Senator Leverett Saltonstall

*I believe in thorough and thoughtful oversight; it distinguished this country from all other countries in the world.*

CIA Director George Tenet

Oversight is a loaded word. When preceded by “Congressional” the term becomes even more loaded for operators in the field. According to Marina Caparini oversight is “supervision, watchful care, management or control.”<sup>1</sup> Applied specifically to the intelligence communities it is “a means of ensuring public accountability for the decisions and actions of security and intelligence communities.”<sup>2</sup> The legislative and executive branches of the US government are engaged in a constant process of balancing against each other. Those in both branches believe they have the best interests of the country at heart but sometimes disagree on how, or the permissible means, to achieve them. The system in place allows Congress to pass laws and convey responsibility to the executive branch to determine the course of action and execute. Congress, however, does not provide the executive with a blank check; it retains the ability to monitor this execution. The tension between legislative and executive branches provides a level of “positive conflict” that is discussed in detail in this chapter. Former House of Representative member Lee Hamilton

---

<sup>1</sup> Marina Caparini, “Controlling and Overseeing Intelligence Services in Democratic States,” in *Democratic Control of Intelligence Services* ed. Hans Born and Marina Caparini (Burlington: Ashgate, 2007), 8.

<sup>2</sup> Hans Born and Loch K. Johnson, “Balancing Operational Efficiency and Democratic Legitimacy,” in *Who’s Watching the Spies?* ed. Hans Born, Loch K. Johnson, and Ian Leigh (Washington: Potomac Books, 2005), 226.

describes this positive conflict best when he said, “Congress must do more than write the laws; it must make sure that the administration is carrying out those laws the way Congress intended.”<sup>3</sup>

### **Congressional Oversight Legislative Overview**

Congressional oversight is not a result of modern scandals as one might think; it is as old as the Constitution itself. In 1788, for example, James Madison laid out how he envisioned the checks and balances of the proposed new government to function in *The Federalist* Number 51.<sup>4</sup> The framers of the Constitution, including Madison, sought to divide the power among the branches of government so they could check one another and then “the private interest of every individual may be a sentinel over the public rights.”<sup>5</sup> Within the Constitution the ‘Necessary and Proper Clause’ in Article I gives Congress the power of oversight of executive branch programs and policies and Article II focuses ‘National Security Power’ in the executive branch.<sup>6</sup> Courts have ruled these Constitutional powers allow the legislative branch to require reports from any executive branch area which can be legislated.<sup>7</sup>

There are many examples of oversight within the government but this thesis focuses specifically on congressional oversight of the intelligence community and the military. The passage of the National Security Act of 1947 ushered in a new era of military and intelligence activity and with it levels of Congressional oversight. Between 1947 and 1974 the oversight was legislated but seldom practiced and relied on mutual confidence between the Executive and Legislative branches.

---

<sup>3</sup> Lee H. Hamilton and Jordan Tama, *A Creative Tension: the Foreign Policy Roles of the President and Congress* (Washington, D.C.: Woodrow Wilson Center Press, 2002), 56.

<sup>4</sup> James Madison, “The Federalist Number 51,” *Independent Journal*, 6 February 1788.

<sup>5</sup> Madison

<sup>6</sup> *U.S. Constitution*, art. I, § .8

<sup>7</sup> Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 4th ed. (Washington: CQ Press, 2009), 205.

Clark Clifford, a former CIA legislative counsel, said of this period that "Congress chose not to be involved and preferred to be uninformed."<sup>8</sup>

The so-called "Era of Trust" that began in 1947 ended abruptly in December 1974 with one article in the New York Times.<sup>9</sup> Seymour Hersh published details of covert actions the Central Intelligence Agency called the "Family Jewels" on December 22, 1974. Public outrage over the details not only sparked heated debate but also led to clamor for Congressional oversight.<sup>10</sup> Hersh began his article with the incendiary sentence, "The Central Intelligence Agency, directly violating its charter, conducted a massive, illegal domestic intelligence operation..." Hersh set Washington ablaze with presidential and congressional inquiries into potential wrong doings; two congressional investigations and one presidential inquiry quickly followed.<sup>11</sup> During the Senate floor debate on passage of the resolution to establish an investigative committee Majority Leader Mike Mansfield said, "It used to be fashionable... for members of Congress to say insofar as the intelligence agencies were concerned, the less they knew about such questions, the better. Well, in my judgment, it is about time that attitude went out of fashion."<sup>12</sup>

With the public's trust potentially broken in late 1974 a new epoch was ushered in, the "Era of Skepticism."<sup>13</sup> Until this time, within intelligence circles viewed trust in the way described by former director of the CIA, Richard Helms: "The nation must to a degree take it on faith that we too are honorable men devoted to her service."<sup>14</sup> No longer would the public, the media, and Congress accept the conditions of the

---

<sup>8</sup> Frank J. Smist, Jr., *Congress Oversees the United States Intelligence Community: Second Edition 1947-1994* (Knoxville: The University of Tennessee Press, 1994), 5.

<sup>9</sup> Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* (Lexington: The University Press of Kentucky, 1985), 253.

<sup>10</sup> Smist, 26.

<sup>11</sup> Seymour M. Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times*, 22 December 1974.

<sup>12</sup> Smist, 50.

<sup>13</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 253.

<sup>14</sup> William Colby and Peter Forbath, *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978), 310.

previous era outlined by Director William Colby: “the nation, in its Congress and press and people, had taken [the legality and morality of intelligence activities] on faith for over twenty years.”<sup>15</sup>

Less than a week after the ink was dry on Hersh’s *New York Times* article, the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961 was signed into law.<sup>16</sup> Originating from over 150 bills presented to Congress over the previous 25 years, this amendment brought congressional oversight to an area viewed as lacking.<sup>17</sup> This landmark legislation not only required the President to be personally involved in covert action decisions but it also required congressional intelligence committees to be fully and currently informed of ongoing activities.<sup>18</sup>

This new legislation, however, did not satisfy the appetite for answers following the Hersh article and potential oversteps by the CIA. On January 4, 1975, President Gerald Ford established the Commission on CIA Activities headed by his Vice President, Nelson Rockefeller, to examine existing measures to prevent violations of provisions within Title 50 of the US Code.<sup>19</sup> In addition to this Commission, the Senate passed a resolution establishing their own committee to investigate these offenses on January 21, 1975.<sup>20</sup> The House of Representatives also passed a resolution to investigate the abuses on their own on February 19, 1975.<sup>21</sup> Within three short months from the article in the *New York Times* three bodies were investigating the intelligence community and the President and Congress enacted legislation making them complicit in all future covert action.

---

<sup>15</sup> Colby 310.

<sup>16</sup> *Foreign Assistance Act of 1961*, Public Law 93-559, 93rd Cong., 2nd sess. (30 December 1974), sec 662.

<sup>17</sup> Senate. *Legislative Proposals to Strengthen Congressional Oversight to the Nation’s Intelligence Agencies: Hearings before the Subcommittee on Intergovernmental Relations*, 93rd Cong., 2<sup>nd</sup> sess., 1974, 1.

<sup>18</sup> *Foreign Assistance Act of 1961*, Public Law 93-559, 93rd Cong., 2nd sess. (30 December 1974), sec 662. And *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947) § 501.

<sup>19</sup> Executive Order 11828, Establishing a Commission on CIA Activities Within the United States, 4 January 1975 and Smist p 27

<sup>20</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 12.

<sup>21</sup> Smist, 135.

Of the three investigative panels formed the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more popularly known as the Church Committee, was the most thorough and impacted Congress and the intelligence community the most. Senator Frank Church (D - ID) led the bipartisan panel along with Senator John Tower (R - TX).<sup>22</sup> Contrary to the party politics of the day the senators ran their committee almost entirely through voice votes and those only where they were absolutely necessary. In doing so Church and Tower avoided more contentious votes that might fracture the committee along party lines.<sup>23</sup> Richard Fenno best describes how this Committee structure, rather than the full Senate, worked best for the investigation into CIA improprieties when he said, “committees are autonomous units, which operate quite independently of such external influences as legislative party leaders, chamber majorities, and the President of the United States.”<sup>24</sup>

As the committee members began their work they faced obstacles thrown at them from all sides. Senator Church felt the weight of the situation as he described his committee’s task, “it is important because there is no more pernicious threat to a free society than a secret police which is operating beyond the law.”<sup>25</sup> First, the Senate resolution creating this committee gave them a task gargantuan in scope. They were to “conduct an investigation and study the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency or by any persons, acting either individually or in combination with others, in carrying out any intelligence or surveillance activities by or on behalf of any agency of the federal government.”<sup>26</sup> Second, the executive branch at all levels stymied the Committee members’ ability to procure

---

<sup>22</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 13-14.

<sup>23</sup> Smist, 35-36, 41.

<sup>24</sup> Richard F. Fenno, Jr., *Congressmen in Committees* (Boston: Little, Brown and Company, 1973), xiii.

<sup>25</sup> Smist, 35.

<sup>26</sup> Smist, 50. Senate, *Congressional Record*, 94th Cong., 1st sess., (21 January 1975), 1432.

documents and testimony for their investigation.<sup>27</sup> Finally, the organizational culture of the main agency on which the investigation focused, the CIA, was not only exceptionally secretive but it had been relatively free of congressional supervision since its establishment in 1947.<sup>28</sup>

After fifteen months, 800 individual interviews, 126 full committee meetings, 40 subcommittee meetings, 250 executive hearings, 21 days of public hearings, and 10,000 pages of documentation the Church Committee made 183 recommendations to the Senate.<sup>29</sup> Its major recommendation was the creation of a permanent intelligence oversight committee but this recommendation was not unanimous.<sup>30</sup> The Committee's vice chairman, Senator Tower, opposed the measure because of the inclusion of defense intelligence assets and said, "I feel that creation of a Select Committee on Intelligence with legislative and authorization authority is the wrong way to do this."<sup>31</sup> Senator Tower's concern highlights the problems inherent in oversight of Title 10 and Title 50. The cross organizational nature of operations elicits problems from overseers organized by agency.

Against Senator Tower's recommendation, on May 19, 1976, the Senate passed Resolution 400 by a margin of 72-22 votes. This Resolution established a Senate Select Committee on Intelligence and thus closed the Era of Skepticism and opened the Era of Uneasy Partnership.<sup>32</sup> This legislation moved oversight from within the armed services committee to this newly formed one and included DoD

---

<sup>27</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 27-36.

<sup>28</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 34.

<sup>29</sup> George B. Lotz, II, "The United States Department of Defense Intelligence Oversight Programme: Balancing National Security and Constitutional Rights," in *Democratic Control of Intelligence Services* ed. Hans Born and Marina Caparini (Burlington: Ashgate, 2007), 112.

<sup>30</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 211, 241.

<sup>31</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 240-241.

<sup>32</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 253, And. Senate, *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94th Cong., 2nd sess., 1976, SR 400. The House later created its own House Select Committee on Intelligence in 1977.

intelligence assets in its purview.<sup>33</sup> It also required annual reports from the heads of the intelligence agencies and broadly defined intelligence activities to include covert and clandestine activities.<sup>34</sup>

The Senate was not the only organization making changes to the way in which the intelligence community went about its business. Earlier in the year President Ford signed Executive Order 11905, which delineated roles and responsibilities for US foreign intelligence activities.<sup>35</sup> He clearly defined the intelligence community and created an executive branch intelligence oversight board to review and vet potentially questionable activities.<sup>36</sup> This order separated special activities from intelligence gathering ones. This subtle line between similar activities would later manifest itself in the line between covert action and clandestine activities. In doing so President Ford created a separate process within the executive branch for approval of these activities and mandated consideration of dissenting opinions during the process.<sup>37</sup> The executive branch recognized the potential for overreach of an agency and attempted to leverage oversight within their branch since it did not exist in significant rigor in the legislative one.

Oversight of intelligence activities remained largely unchanged until 1980 when another event changed the calculus in the minds of those in Congress. A stipulation of the Hughes-Ryan Amendment required the President, among others, to brief an inordinate number of committees prior to any covert action. This significantly limited the flexibility and speed of the executive branch to respond to emerging crises using covert means. When confronted by a continuing hostage crisis in Iran, President Jimmy Carter elected not to notify members of

---

<sup>33</sup> Johnson, *A Season of Inquiry: The Senate Intelligence Investigation*, 174.

<sup>34</sup> S. Res 400, 94th Con., 2nd sess., 1976.

<sup>35</sup> Executive Order 11905, United States Foreign Intelligence Activities, 18 February 1976.

<sup>36</sup> EO 11905, United States Foreign Intelligence Activities.

<sup>37</sup> EO 11905, United States Foreign Intelligence Activities.

Congress about a proposed military hostage rescue attempt in April.<sup>38</sup> In response to the dramatic failure of the mission, code named “Eagle Claw,” but more importantly the executive’s attempt to subvert its authority Congress amended the provision of Hughes-Ryan and replaced it with language directly added to Title 50 USC.<sup>39</sup>

As part of the Intelligence Authorization Act for Fiscal Year 1981, Congress amended Title 50 to include a section entitled, “Accountability for Intelligence Activities.”<sup>40</sup> In this provision they established two levels of executive notification to Congress based on a presidential determination of risk. To give back the executive some of its freedom of action Congress agreed to reduce the number of committees fully informed to only the intelligence committees of both houses.<sup>41</sup> The provisions of this Act under Title 50 gives the President the ability when “under extraordinary circumstances affecting vital interests of the United States” to notify only the leadership of the intelligence committees and houses of Congress until these circumstances pass.<sup>42</sup> The leadership mentioned in this statute became the “the Gang of Eight.”<sup>43</sup> This limited reporting mechanism made it more palatable for executive branch officials to keep Congress informed of covert action activities.

To restore freedom of action to both the CIA and the executive branch President Ronald Reagan signed Executive Order 12333<sup>44</sup> shortly after taking office in 1981. This Order designated the role for each of the intelligence agencies and defined the purpose of the intelligence effort.<sup>45</sup>

---

<sup>38</sup> Smist, 96.

<sup>39</sup> Smist, 96, *Intelligence Authorization Act for 1981*, Public Law 96-450, 96th Cong., 2nd sess., (14 Oct 1980), Title V.

<sup>40</sup> *Intelligence Authorization Act for 1981*, Title V.

<sup>41</sup> *Intelligence Authorization Act for 1981*, Title V.

<sup>42</sup> *Intelligence Authorization Act for 1981*, Title V.

<sup>43</sup> Eric Rosenbach and Aki J. Peritz, *Trials by Fire, Counterterrorism and the Law* (Cambridge: Belfer Center for Science and International Affairs, 2010) 38.

<sup>44</sup> Executive Order 12333, United States Intelligence Activities, 4 December 1981. EO 12333 is the landmark EO for intelligence. It defines roles and responsibilities as well as specific procedures for covert action in conjunction with Title 50.

<sup>45</sup> EO 12333 United States Intelligence Activities.

The US intelligence effort “shall provide...the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats.”<sup>46</sup> In the expanded roles and responsibilities of intelligence agencies the Order delineates who should have execution authority and under what conditions organizations can participate in covert action.<sup>47</sup> The definition of covert action matches the one used in Title 50 USC. Most importantly, the Order explicitly states that the President is the only person who can issue a finding for covert action.<sup>48</sup> During President Reagan’s tenure, however, members of Congress believed that he had overstepped his authority in the so-called “Iran-Contra affair.” The scandal involved the covert sale of arms, specifically spare parts, to fund the arming of Contra guerrillas in Nicaragua. At issue was the fact that Reagan used executive authorities and covert means to outmaneuver a specific Congressional ban on support to the Contras.

The final piece of legislation affecting modern congressional oversight of the intelligence community occurred directly as a result of the Iran-Contra affair: the 1991 Intelligence Authorization Act. In the investigation following Iran-Contra, members of Congress learned that the Reagan Administration had followed the letter of law by making the necessary “Gang of Eight” notifications. Members of Congress felt this was not the intention of the legislation, or the spirit of the law, so they clarified the provision and provided procedures for its future use.<sup>49</sup> The 1991 Act levies four requirements on the President in the event he or she chooses to use the limited reporting option. First, the President must provide a reason for limiting reporting such as risk to life. Second, the

---

<sup>46</sup> EO 12333 United States Intelligence Activities.

<sup>47</sup> EO 12333 United States Intelligence Activities.

<sup>48</sup> EO 12333 United States Intelligence Activities.

<sup>49</sup> Alfred Cumming, *Sensitive Covert Action Notifications: Oversight Options for Congress*, CRS Report for Congress (Washington: Congressional Research Service, Sept 25, 2009), 4.

two chairmen of the intelligence committees must sign the finding. Third, the notification must be prior to the start of the covert action to allow Congress time to provide alternatives. Finally, the “Gang of Eight” must receive updates on any changes to the authorized action.<sup>50</sup>

Overall the 1991 Act provides a middle ground between those desiring less reporting, to allow greater freedom of action, and those who believe that covert action requires more oversight and accountability. Since the passage of the 1991 Act there have been attempts by individual committees to modify this limited reporting option; so far though, nothing has changed.<sup>51</sup> Within Congress some contend oversight, as currently conducted, does not offer them the ability to approve or disapprove covert actions.<sup>52</sup> They also contend the information provided is so limited they cannot make informed decisions or even understand the information presented to them.<sup>53</sup> The statutory restriction on taking notes or discussing the matter with their colleagues limits their ability to provide oversight. Finally, many complain the limited reporting mechanism is overused.<sup>54</sup>

### **Contemporary Oversight**

Two models explicate congressional oversight of the executive branch. The first is institutional and the second is investigative.<sup>55</sup> In the institutional model Frank Smist asserts oversight is a cooperative endeavor which relies on the attitudes of members of the executive and legislative branch to dictate its character.<sup>56</sup> Investigative oversight,

---

<sup>50</sup> *Intelligence Authorization Act for Fiscal Year 1991*, Title VI.

<sup>51</sup> *Intelligence Authorization Act for Fiscal Year 1991*, Title VI.

<sup>52</sup> *Intelligence Authorization Act for Fiscal Year 1991*, Title VI.

<sup>53</sup> *Intelligence Authorization Act for Fiscal Year 1991*, Title VI.

<sup>54</sup> *Intelligence Authorization Act for Fiscal Year 1991*, Title VI.

<sup>55</sup> Smist, 20 and Loch K. Johnson, “Governing in the Absence of Angels,” in *Who’s Watching the Spies?* ed. Hans Born, Loch K. Johnson, and Ian Leigh (Washington: Potomac Books, 2005), 59. The authors use different terms to describe the same phenomena, Johnson uses police patrolling and fire fighting instead.

<sup>56</sup> Smist, 21

however, reflects a more adversarial relationship between the two branches.<sup>57</sup>

Institutional oversight is not without problems though. The potential exists for individual members of Congress to be co-opted by the agency they are charged with overseeing making it difficult for them to remain objective.<sup>58</sup> To defend against this, the Senate limits the length of time Senators can serve on the intelligence committee.<sup>59</sup> Another condition for effectiveness is that executive agencies must be forthright with information and testimony to maintain trust.<sup>60</sup> Agency directors sometimes cite Congress as responsible for the most intelligence leaks but the data does not support this.

The committees responsible for intelligence oversight perform differently than other committees in Congress because oversight is their main function rather than a secondary one. For these committees to be effective both methods of oversight must occur simultaneously.<sup>61</sup> An external event, such as a media report or public failure, usually triggers the investigative or firefighting model.<sup>62</sup> In this instance the oversight becomes more pronounced and intrusive making it more difficult for the executive branch to accomplish programs. This is why they attempt to keep the majority of oversight within the institutional bounds.

### **How is Oversight Accomplished**

Using control of the budget, hearings, nominations, reports, and investigations Congress maintains oversight.<sup>63</sup> These are the levers available to members of the legislative branch to force answers and or actions from an agency. All of the levers are not of equal length and not

---

<sup>57</sup> Smist, 22.

<sup>58</sup> Johnson, "Governing in the Absence of Angels," 72.

<sup>59</sup> S. Res 400, 94th Con., 2nd sess., 1976.

<sup>60</sup> Johnson, "Governing in the Absence of Angels," 69-70.

<sup>61</sup> Smist, 23.

<sup>62</sup> Johnson, "Governing in the Absence of Angels," 59.

<sup>63</sup> Lowenthal, 4th ed., 205-212.

all of the oversight functions for the intelligence community fall inside the intelligence committees, specifically budgetary actions.

The budget lever is one of the largest and most important for the intelligence community. For a particular program within the US budget process there are authorizations and appropriations, both of which are required prior to money changing hands. The respective intelligence oversight committees handle authorizations; the defense subcommittees of the respective appropriations committees oversee appropriations.<sup>64</sup> These functions are separate by design to guarantee accountability. This process provides Congress with a way to inject impediments to programs or not allow actions within a particular area of the world if it so chooses.

The oversight committees use hearings, reports, and investigations to elevate their voices. The current laws regarding covert action do not allow Congress to vote yes or no but by calling hearings, requesting reports or launching investigations its members can put pressure on the executive branch. Congress can do so by publicizing the details of actions, or forcing executive officials to provide rationale or defend the actions they have taken. Such concerns and details then become part of the public record, accessible to all and potentially broadcast by the media. Fear that publicity can turn the public against its elected executive is one way Congress can constrain an administration from taking a particular action. In the past such instances prevented administrations from pursuing policies aiding the Nicaraguan contras.<sup>65</sup> In addition, once the press exposed the details of Iran-Contra to the public President Reagan's popularity plummeted by more than 20 points.

The final method of enacting oversight is through Senate confirmation of intelligence community political appointees. This method has often been the most controversial lever for action within the legislative branch but an effective one nonetheless. Critics maintain this

---

<sup>64</sup> Lowenthal, 4th ed., 205-206.

<sup>65</sup> Lowenthal, 4th ed., 208.

process has become too political and things irrelevant to nominees' ability to perform duties have become grounds for no votes.<sup>66</sup> On the other hand this power in the Senate has allowed them to prevent individuals responsible for unpopular policies from promotion to higher positions.<sup>67</sup>

### **Titles 10 and 50 of the U.S. Code**

Congressional oversight is a delicate enough subject as it reconciles the attempts of two separate branches of government to solve problems. The specific oversight discussed in this thesis though is more complex because it also spans multiple organizational and agency lines.

Two sections of United States Code (U.S. Code) divide the laws governing the application of military force and covert action. This division and its interaction with Congress is the second part of this examination. In part this study will answer why the division exists, what the division means for policy makers, and how operations occur in and between these divisions.

Prior to the National Security Act of 1947 the laws governing the US military were spread between Title 10 (the Army), Title 34 (the Navy), and Title 50 (war making).<sup>68</sup> Following the Act's passage and reforms in 1956 the Titles became Title 10 (Armed Forces) and Title 50 (War and National Defense).<sup>69</sup> The headings are somewhat misleading however. The goal of the National Security was to combine all military departments into one under the leadership of the Secretary of Defense. The preponderance of the Secretary's authorities is contained in Title 10 but

---

<sup>66</sup> Lowenthal, 4th ed., 209.

<sup>67</sup> Lowenthal, 4th ed., 210.

<sup>68</sup> 10 U.S.C. (1956), 50 U.S.C. (1917), And *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947)

<sup>69</sup> *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947), 10 U.S.C. (1956), And 50 U.S.C. (1917)

with the creation and consolidation of an intelligence community those authorities moved to another title, Title 50.<sup>70</sup>

The titles now form the basis for division of labor within the military and intelligence communities as well as committees within Congress. Since the Secretary of Defense, unlike other members representing both groups, supervises the armed forces and the intelligence community his or her authority resides in both statutes creating confusion. These titles created artificial boundaries that over time led to a degree of specialization not conceived of in 1947.

The main focus of this thesis is to examine how these artificial boundaries, regarding action and intelligence, generate unnecessary angst within the government by examining the characteristics of three major categories, covert action, clandestine activities, and traditional military authority.

### **Characteristics of Covert Action, Clandestine Activities, and Traditional Military Authorities**

Covert action, clandestine activities and traditional military authority, defined in the Introduction, have many distinguishing characteristics. Analytically one can separate these characteristics as follows: developers, execution authorities, legal authorities, congressional oversight, implications, deniability, and command. Table 1 on the following page graphically simplifies and depicts, as well as provides a framework for analysis of, the relationship between actors, acts, and authorities. The remainder of Chapter One explains the analytic significance of some of the more pertinent differences between these distinguishing characteristics.

---

<sup>70</sup> *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947).

**Table 1: Characteristics**

	<b>Covert Action</b>	<b>Clandestine Activity</b>	<b>Traditional Military Activity</b>
<b>Developer</b>	NSC	Military/Agency Director	Military/Agency Director
<b>Execute Authority</b>	President	SecDef/COCOM <sup>1</sup>	SecDef/COCOM <sup>1</sup>
<b>Oversight</b>	Intelligence Committee	Armed Services/ Other	Armed Services
<b>Legal Authority</b>	Title 50/ EO 12333	Title 10/50 EO12333	Title 10
<b>Deniability</b>	Sponsor	Act	None
<b>Policy Basis</b>	CIA	Agency	Military
<b>Command</b>	CIA	Military/Agency Director <sup>2</sup>	Military

<sup>1</sup> President or SecDef must approve SOCOM missions (PL 108-136)

<sup>2</sup> Agency directors may supervise their own missions if they are conducting clandestine operations.

*Source: Author's Original Work*

### **Development**

Foreign policy frequently has many fathers but this is never the case with covert action. Section 413b of Title 50 USC gives sole responsibility to the President to approve covert action through a written finding.<sup>71</sup> In Executive Order 12333 (EO 12333)<sup>72</sup> the President charges the National Security Council (NSC) with preparing all policy recommendations that consider covert action and further requires them to include the dissenting and assenting opinions in their recommendation.<sup>73</sup> The Executive Order also states, “The NSC shall act as the highest ranking executive branch entity that provides support to

<sup>71</sup> 50 U.S.C. § 413b

<sup>72</sup> Executive orders and presidential directives are not law but carry the force of law when made within the authority of act of congress that gives the president discretionary power.

<sup>73</sup> EO 12333 United States Intelligence Activities.

the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.”<sup>74</sup> These authorities make the NSC, with its attendant membership, the developer of all covert action programs.

U.S. Code uses the word “clandestine” numerous times but does not define it. The definition used previously comes from DoD publications. Without a clear, codified definition individual agencies can define it themselves. This room for interpretation is also room for exploitation. Since 1986, with the passage of the Goldwater-Nichols Defense Reorganization Act, Combatant Commanders (COCOMs) as well as agency directors develop clandestine activities plans. Operations with the clandestine moniker are not limited to DoD forces. EO 12333 and Title 50 USC allow for intelligence collection via clandestine methods.<sup>75</sup>

### **Execute Authority**

The authority to execute covert action missions rests solely with the President. Title 50 Section 413(b) states “The President may not authorize the conduct of a covert action by departments, agencies, or entities of the United States Government unless the President determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.”<sup>76</sup>

Clandestine activities have varied execute authorities. Title 50 discusses clandestine collection of intelligence by members of the defined intelligence community.<sup>77</sup> The agency director, if a non-DoD agency, authorizes clandestine activity. Within the DoD the Secretary of Defense or geographic combatant commander can authorize clandestine missions

---

<sup>74</sup> EO 12333 United States Intelligence Activities.

<sup>75</sup> 10 U.S.C. (1956) and EO 12333 United States Intelligence Activities.

<sup>76</sup> 50 U.S.C. § 413b

<sup>77</sup> 50 U.S.C. (1917)

with the exception of US Special Operations Command (SOCOM).<sup>78</sup> Recognizing SOCOM's global domain and extensive reach in the war on terrorism, Congress stipulated the President or Secretary of Defense must approve all SOCOM missions as part of the Defense Authorization Act in 2004.<sup>79</sup>

### **Oversight**

The intelligence committees in Congress provide oversight for all covert action missions as discussed previously. Title 50 USC Section 413(b) is explicit in both its definition and oversight requirements. Regardless of who executes the covert action they are the oversight authority.

Clandestine missions are subject to oversight from the appropriate committee overseeing their department. The armed services committee in the House and Senate provide oversight to the military, while National Security Agency clandestine collection missions receive oversight from the intelligence committees.

Traditional military activities are just those— activities in which the military traditionally participates. The covert action definition provides an exception for all items classified as traditional military tasks.<sup>80</sup> The armed services committees handle oversight of traditional military activity.

### **Legal Authority**

Title 50 USC and EO 12333 contain the legal authority to conduct covert action. Title 50 provides the broad reasons and procedures for who can conduct covert action.<sup>81</sup> EO 12333 explicitly breaks down who can conduct covert action and under what conditions they can do so.<sup>82</sup>

---

<sup>78</sup> 10 U.S.C. (1956)

<sup>79</sup> *National Defense Authorization Act for 2004*, Public Law 108-136, 108th Cong., 1st sess. (24 November 2003), §904.

<sup>80</sup> 50 U.S.C. § 413b

<sup>81</sup> 50 U.S.C. (1917)

<sup>82</sup> EO 12333 United States Intelligence Activities.

For example it states the military can only perform covert action missions during declared war or another action covered under the War Powers Resolution.<sup>83</sup>

Title 10, Title 50, and EO 12333 all discuss clandestine activities and offer the legal authority to conduct them. The broad clandestine umbrella term forces the legal authorities' inclusion in both titles and the EO. Many different organizations conduct these operations so the authorities are several places. Traditional military activity is just that so the authority is in Title 10 U.S. Code.

### **Deniability**

Deniability is a major concern of these types of operations. Covert operations hide the sponsor of the organization but may not hide the operation itself.<sup>84</sup> While clandestine operations hide the act while not denying the perpetrator.<sup>85</sup>

This deniability was a strong consideration in the legislation creating Title 50 Section 413(b) as it is today. Members of Congress and CIA employees were concerned by requiring the President to authorize all findings in writing they may be removing this deniability. The events following the Iran-Contra scandal elevated the need for oversight above the need for deniability however.

### **Policy**

Title 50 USC Section 413(b) is specific about few things outside of oversight but one thing it mentions explicitly is policy guidance. It directs all agencies conducting covert action to use CIA policy guidance if they do not have approved guidance of their own.<sup>86</sup> This de facto established the CIA as the lead agency for all covert action. The laws and executive orders do make the same stipulations for clandestine activities.

---

<sup>83</sup> EO 12333 United States Intelligence Activities.

<sup>84</sup> Joint Publication 3-05.1 *Joint Special Operations Task Force Operations*, 26 April 2007 GL-10.

<sup>85</sup> Joint Publication 3-05.1 *Joint Special Operations Task Force Operations*, GL-10.

<sup>86</sup> 50 U.S.C. § 413b

## **Command**

The final characteristic considered is command. The CIA is capable and legal to be in command of a covert action even it uses military forces in its execution as occurred in Operation NEPTUNE'S SPEAR to kill Osama bin Laden.<sup>87</sup> In Senate Report 102-85 members used command as a discriminator to determine if an operation was covert action or not. Members of the Senate said traditional military activity includes operations under the control of a US military commander (whether or not the US sponsorship of such activities is apparent or later acknowledged.)<sup>88</sup> Command of the operation therefore can possibly determine the entire string of other characteristics to which an operation is subject.

## **Conclusion**

This chapter spent considerable time discussing the history of congressional oversight to demonstrate how oversteps of authority have led to the system in place today. As a result of these overreaches tighter scrutiny descended upon military and intelligence activities. The lesson is that avoiding these miscues can prevent increased scrutiny in the future.

The key to avoiding these mistakes is to understand the complex legal environment in which the military and intelligence communities operate today. The characteristics of covert action, clandestine activities and traditional military activity discussed provide a discussion framework and attempt to avoid confusion caused by terminology misuse. A policy maker operating in this realm must be familiar with the lines between agencies and authorities to be accurate and effective.

---

<sup>87</sup> Marc Ambinder and D.B. Grady, *The Command: Deep Inside the President's Secret Army*. (Hoboken: John Wiley & Sons, 2012) location 139-143.

<sup>88</sup> Senate, *Authorizing Appropriations for Fiscal Year 1991 For the Intelligence Activities of the U.S. Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System and for Other Purposes*, 102nd Cong., 1st sess., 1991, SR 102-85, 44.

## CHAPTER 2

### SOCOM AND THE CIA

*...while the U.S. [military] teams operated clandestinely, they did not engage in covert action.*

Stephen Cambone, Under Secretary of Defense for Intelligence, in testimony to Congress

The CIA and the military have not always enjoyed the collegial relationship exemplified today in the war on terror.<sup>1</sup> Starting in 1947 with the creation of the CIA there has been tension over paramilitary operations because the direct action element so closely resembles military action. Further complicating matters, in the aftermath of Operation EAGLE CLAW, the failed American hostage rescue attempt in Iran, Congress created US Special Operations Command (SOCOM) to develop mature special operations capability to be on call for military use. These seemingly similar organizations worked hard to maintain their distinctiveness over the years.

#### **A Budding or Head-Butting Relationship**

The authors of the National Security Act of 1947 took on a herculean task. This legislation created the Department of Defense, the National Security Council, and the Central Intelligence Agency.<sup>2</sup> Even more difficult than creating these institutions was the task of dividing out the responsibilities of each of these new agencies, as well as committees to oversee them. Congress created Title 10 and Title 50 to help them separate the authorities of the new departments and agencies.

One of the authorities Congress placed within Title 50 was for covert action. The Truman Administration struggled over which

---

<sup>1</sup> Steven Emerson, *Secret Warriors: Inside the Covert Military Operations of the Reagan Era*, (New York: G.P. Putnam's Sons, 1988), 7-11.

<sup>2</sup> *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947).

organization to give covert action authorities.<sup>3</sup> During the World War II, both the military and the newly created Office of Strategic Services (OSS) conducted numerous covert action operations by today's definitions. After the war, however, none of the service chiefs wanted that authority.<sup>4</sup> Senior leaders within DoD viewed covert action as an alternative to military action and they did not believe that both activities should be conducted by the same organization in 1947.<sup>5</sup> Those leaders were also concerned that if they conducted covert action, it could potentially cause problems for related to plausible deniability of their actions for the United States.<sup>6</sup>

The debate over covert action authorities lay largely dormant until 1980 when the failure to rescue Americans held hostage in Tehran, coupled with confusion and overlapping activities in Grenada during Operation URGENT FURY, led Congress to the establish SOCOM in 1987.<sup>7</sup> With the creation of SOCOM the military appeared to possess a covert action force. Those within Congress tried to allay fears within the CIA that the military would take over paramilitary operations by including within Title 10 the stipulation that the creation of SOCOM does not, "constitute authority to conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require notification" to the intelligence committees.<sup>8</sup>

The explicit text of Title 10 did not unequivocally separate SOCOM and CIA authorities and confusion and room for interpretation persisted. Lawyers within SOCOM argued that the Command's approved military doctrine and unit training provided authority to execute missions clandestinely. Lawyers within the Pentagon's Office of General Council

---

<sup>3</sup> William J. Daugherty, *Executive Secrets: Covert Action and the Presidency*, (Lexington: The University Press of Kentucky, 2004), 59.

<sup>4</sup> Daugherty, 59.

<sup>5</sup> Mark M. Lowenthal, *Intelligence: from Secrets to Policy*, 2nd ed. (Washington, D.C.: Cq Pr, 2003), 134.

<sup>6</sup> Lowenthal, , *Intelligence: from Secrets to Policy*, 2nd ed, 134.

<sup>7</sup> 10 U.S.C § 167

<sup>8</sup> 10 U.S.C. § 167 (g)

(OGC) disagreed with SOCOM's argument. The OGC lawyers, using a broad interpretation of the definitions within Title 50, said that any attempt to plausibly conceal the US as an actor made the operation covert action and not clandestine.<sup>9</sup> The crux of the debate according to one Defense official was cultural; the majority opinion was that DoD did not have the authority to execute covert action missions because it did not want the authority.<sup>10</sup>

William Daugherty, a former CIA employee, lists four reasons why the military should not possess covert action authorities in his book *Executive Secrets*. First he mentions the military does not have explicit authorities in US law to conduct covert action.<sup>11</sup> The military does, however, have implicit authorities. For example, within EO 12333, the President does not limit covert action to the CIA and states the military may be lead agency in time of war.<sup>12</sup> Secondly Daugherty states it is easier for the CIA than the military to conceal US sponsorship.<sup>13</sup> Third he brings up another legal argument; the CIA often uses third-party nationals to conduct operations, which enhances deniability. While Congress does not prohibit the military from employing proxies, its personnel must do so in uniform and carry identification according to the Law of Armed Conflict (LOAC).<sup>14</sup> Fourth, Daugherty points out that the CIA has a presence in over 190 embassies throughout the world with personnel fluent in the local languages and culture.<sup>15</sup> These four reasons were enough to keep the operations of both SOCOM and the CIA largely separate, except for occasional support to each other, until 9/11.

---

<sup>9</sup> Richard H. Shultz, Jr., "Showstoppers," *The Weekly Standard* 9, no. 19, 26 January 2004, <http://www.weeklystandard.com/Content/Public/Articles/000/000/003/613twavk.asp>.

<sup>10</sup> Shultz.

<sup>11</sup> Daugherty, 61.

<sup>12</sup> Executive Order 12333, United States Intelligence Activities, 4 December 1981.

<sup>13</sup> Daugherty, 61.

<sup>14</sup> Daugherty, 61.

<sup>15</sup> Daugherty, 62.

### **Title 10/50 Post-9/11**

On September 13, 2001, as most of America was still reeling from the 9/11 attacks, CIA Director George Tenet and Secretary of Defense Donald Rumsfeld briefed President George Bush on options to respond to the terrorist attacks two days prior. The course of action selected by the President placed Special Forces with CIA teams to dislodge the Taliban from power. By September 17, 2001 President Bush gave the order authorizing the action and told Tenet, “I want the CIA to be first on the ground.”<sup>16</sup> This forced the CIA and DoD to work together closely and this led to a number of problems and tensions.

The CIA and DoD operate under different authorities, as already discussed above, and this caused “a lot of bureaucratic tension.”<sup>17</sup> As the relationship matured there were constant questions about who was in charge. To expedite the deployment and employment of Special Forces teams, Secretary Rumsfeld signed operational control for them over to the CIA although he was not happy about doing so.<sup>18</sup> Secretary Rumsfeld believed that the CIA operatives would migrate to DoD control once the special operators were in place. Director Tenet had exactly the opposite opinion.<sup>19</sup> Eventually covert and clandestine operators remained under the control of their own organizations with neither commanding or controlling the other.

When the 9/11 Commission reported out in 2004 its members offered Congress and the President with a recommendation to address this problem of authorities. Commission members recommended that the “lead responsibility for directing and executing paramilitary

---

<sup>16</sup> George Tenet with Bill Harlow, *At the Center of the Storm: My Years at the CIA* (New York: Harper, 2007), 208.

<sup>17</sup> Tenet, 215.

<sup>18</sup> Bradley Graham, *By His Own Rules*, (New York: PublicAffairs, 2009), 585.

<sup>19</sup> Donald Rumsfeld, *Known and Unknown*, (New York: The Penguin Group, 2011), 375; Tenet, 215-216.

operations, clandestine or covert, should shift to the DoD.”<sup>20</sup> In the discussion leading up to this recommendation they lauded the CIA-military teams for their success in Afghanistan and suggested that future cooperation should be included in exercises.<sup>21</sup> The Commission’s report partially explains this dichotomy in statements highlighting the supposed strengths and weaknesses of both organizations but does little to offer a way to achieve their recommendation. Observers of the Commission’s deliberations suggest senior leaders of DoD lobbied for this recommendation in order to take over responsibility and authority for paramilitary covert action.<sup>22</sup>

The CIA and SOCOM share some similar roles and missions but these derive from their separate authorities from different sources. One can best depict graphically these authorities and their sources for better understanding their overlaps. The following table (Table 2) illustrates how the CIA and SOCOM authorities are similar and different.

---

<sup>20</sup> National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States*. (New York: W. W. Norton & Company, 2004), 415.

<sup>21</sup> National Commission on Terrorist Attacks, 416.

<sup>22</sup> Gary Berntsen, *Human Intelligence, Counterterrorism, & National Leadership*, (Washington, D.C.: Potomac Books, 2008), 43 and Seymour Hersh, “The Gray Zone,” *The New Yorker* (24 May 2004)

**Table 2: Characteristics (CIA & SOCOM)**

	<b>Covert Action</b>	<b>Clandestine Activity</b>	<b>Traditional Military Activity</b>
<b>Developer</b>	NSC	Military/Agency Director	Military/Agency Director
<b>Execute Authority</b>	President	SecDef/COCOM <sup>1</sup>	SecDef/COCOM <sup>1</sup>
<b>Oversight</b>	Intelligence Committee	Armed Services/ Other	Armed Services
<b>Legal Authority</b>	Title 50/ EO 12333	Title 10/50 EO12333	Title 10
<b>Deniability</b>	Sponsor	Act	None
<b>Policy Basis</b>	CIA	Agency	Military
<b>Command</b>	CIA	Military/Agency Director <sup>2</sup>	Military

<sup>1</sup> President or SecDef must approve SOCOM missions (PL 108-136)

<sup>2</sup> Agency directors may supervise their own missions if they are conducting clandestine operations.

*Source: Author's Original Work*

### **Developer and Command**

EO 12333 requires the NSC to develop the plans for all covert action but SOCOM missions are often high risk/high reward missions generated at upper levels of the government as a result of crisis action planning.<sup>23</sup> This different risk/reward calculus—long-term covert action versus near-term, but potentially high-payoff clandestine action—means that the component level plans the missions but the NSC receives a brief before the President makes an execution decision. The EAGLE CLAW mission to rescue Americans held hostages in Iran occurred this way even before SOCOM existed. The mission was not covert action as is popularly depicted; rather the military executed Operation EAGLE CLAW

<sup>23</sup> EO 12333 United States Intelligence Activities.

as a clandestine operation.<sup>24</sup> A small organization in the bowels of the Pentagon planned and rehearsed this complex mission before asking President Jimmy Carter for the execute order.

A major part of a decision on whether a mission should be covert or clandestine is who commands it. EO 12333 stipulates that the CIA will be in command for covert action in all circumstances other than wartime, at which point the military can command.<sup>25</sup> Operation NEPTUNE'S SPEAR (the raid that killed Osama bin Laden in Abbottabad, Pakistan in May 2011) was a covert action; then-CIA Director Panetta was in overall command of the mission.<sup>26</sup> The close working relationship that the CIA and SOCOM enjoy today allows policy makers to make decisions about covert action or clandestine activities based on oversight and secrecy requirements. While this relationship works well for the operators the ability to move seamlessly back and forth between covert and clandestine is detrimental to oversight. The executive branch should inform Congress whether missions are clandestine or covert; oversight should not be the reason to select clandestine or covert over the other.

### **Oversight - Capability Creep**

On September 11, 2001, SOCOM was a supporting command meaning it merely provided forces for geographic combatant commanders to use.<sup>27</sup> The warfighters up until this time were those geographic combatant commanders charged with regional areas of responsibility, with all other major and unified commands designed to support them. General Charles Holland (USAF), commander of SOCOM on and after 9/11, was reluctant to engage terrorists outside this command construct. Secretary Rumsfeld, however, wanted action and he pushed

---

<sup>24</sup> Emerson, 12.

<sup>25</sup> EO 12333 United States Intelligence Activities.

<sup>26</sup> Eric Schmitt and Thom Shanker, *Counterstrike*, (New York: Times Books, 2011), 258-261.

<sup>27</sup> US Special Operations Command, "History United States Special Operations Command, 6<sup>th</sup> ed. 31 March 2008," US Special Operations Command, <http://www.socom.mil/Documents/history6thedition.pdf>, (accessed 19 March 2012) 12.

for SOCOM to receive global authorities.<sup>28</sup> In 2004, Secretary Rumsfeld and the Chairman of the Joint Chiefs submitted an updated Unified Command Plan with SOCOM designed as a supported command for the “Global War On Terrorism.”<sup>29</sup> In this capacity SOCOM can plan and execute missions like a geographic combatant commander without the latter’s input or knowledge.<sup>30</sup>

This expansion of SOCOM authorities came to the attention of some members of Congress and in 2004 they added a provision to the Defense Authorization Act that added a layer of executive branch oversight. The Act stipulates either the Secretary of Defense or the President must approve all SOCOM missions.<sup>31</sup> This provision made newly-appointed Secretary of Defense Robert Gates more comfortable with the authority granted to SOCOM. He placed further restrictions on the command: all lethal counterterrorism missions had to be approved by the President unless they met more stringent, time sensitive requirements.<sup>32</sup> These types of authorities closely resemble the authorities that Congress granted the CIA, although the oversight for these Title 10 missions remained within the armed services committee. This *de facto* change to Title 10 authorities placed SOCOM clandestine mission execution decisions on the same level as ones for CIA covert action.

The members of the two Intelligence Committees witnessed this change in SOCOM authorities with apprehension. The new authorities so closely resemble covert action that Committee members wanted increased oversight of the operations. The Intelligence Committees legislated that SOCOM produce a “Clandestine Quarterly” to ensure its

---

<sup>28</sup> Graham, 370.

<sup>29</sup> *History United States Special Operations Command*, 6<sup>th</sup> ed. 31 March 2008, 15-16.

<sup>30</sup> Jennifer D. Kibbe, “The Rise of the Shadow Warriors,” *Foreign Affairs* (March/April 2004) 103.

<sup>31</sup> *National Defense Authorization Act for 2004*, Public Law 108-136, 108th Cong., 1st sess. (24 November 2003), §904.

<sup>32</sup> Schmitt and Shanker, 246.

members were aware of recent DoD clandestine missions.<sup>33</sup> The report only covers clandestine activities that are already completed and SOCOM produces it on a quarterly basis so its information could be as old as three months. While the publishing of the Clandestine Quarterly provides Congress with a level of oversight it is nevertheless ineffective. Oversight is about responsibility for, accountability of extraordinary powers before, and while they are being used; Congress cannot accomplish effective oversight in hindsight.

As SOCOM's forces have expanded in the last decade so have those of the CIA. Although specific numbers are classified, open source estimates place the number of covert action operators (as opposed to case officers and analysts) in the CIA after 9/11 at around 600-700 while SOCOM has approximately 10,000 operators or "trigger pullers."<sup>34</sup> This disparity in the number of operators means that the CIA must often ask SOCOM to augment its personnel.<sup>35</sup> During declared hostilities this poses little risk to the operators themselves. However in the dynamic environment of covert action in areas outside designated zones of conflict military members submit themselves to increased risk. While operating with the CIA, the military members may have to forfeit protections normally guaranteed to them by the Geneva Conventions.<sup>36</sup> In recent years SOCOM has grown significantly and one can assume that the number of Clandestine Service CIA paramilitary personnel has also increased.<sup>37</sup>

Although the granting of additional authorities and the expansion in the number of personnel eased the ability of operators to coordinate in the field, they managed to exacerbate tensions between SOCOM and the

---

<sup>33</sup> The author has firsthand knowledge of this reporting requirement but has not been able to uncover the specific legislation requiring its production.

<sup>34</sup> Kibbe, "The Rise of the Shadow Warriors," 112.

<sup>35</sup> Kibbe, "The Rise of the Shadow Warriors," 112.

<sup>36</sup> Kibbe, "The Rise of the Shadow Warriors," 113.

<sup>37</sup> The informal name of "Clandestine Service personnel" by the CIA further complicates an already murky distinction between clandestine (Title 10) and covert action (Title 50).

CIA. These tensions resulted in a “turf war” between Secretary Rumsfeld and Director Tenet when they ran DoD and CIA respectively.<sup>38</sup> This conflict worked its way throughout their different bureaucracies and gave rise to discussions about which organization should be the executive agent for covert action. Following Rumsfeld and Tenet’s retirement from public service such discussions have virtually disappeared from the press. If anything, stories in the press and professional journals laud the degree of recent interagency cooperation.<sup>39</sup> This is not to say that tensions and “turf wars” do not still exist but merely that they have largely faded from media attention and scholarly discourse.

### **Policy Basis - Muddy Water and the AUMF**

In the immediate aftermath of the 9/11, leaders framed the attacks in a context of criminal acts.<sup>40</sup> Within a few days the President modified his previous statements and began discussing the attacks as an act of war. This subtle difference in syntax dramatically changed how America responded. On September 14, 2001, both branches of Congress passed the Authorization to Use Military Force (AUMF) and on September 18 President Bush signed it into law.<sup>41</sup> The law is a simple piece of legislation comprised of a single sentence: “The President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.”<sup>42</sup>

---

<sup>38</sup> Kibbe, Hersh, Graham, Tenet, and Rumsfeld all describe the fight for control during this time period. Once these players left the stage the discussion calmed down but still deserves mention.

<sup>39</sup> See for example Christopher Lamb and Evan Munsing, *Secret Weapon: High-value Target Teams as an Organizational Innovation*, Strategic Perspectives No. 4 (Washington, DC: NDU Press, March 2011).

<sup>40</sup> Kibbe, “The Rise of the Shadow Warriors,” 109.

<sup>41</sup> *Authorization to Use Military Force*, Public Law 107-40, 107th Cong., 1st sess. (14 September 2001).

<sup>42</sup> *Authorization to Use Military Force*, 14 September 2001.

This is the first time Congress authorized action against a non-state entity (i.e., a person, group, or organization) as opposed to a state.<sup>43</sup> The Authorization represents a cessation of power from Congress to the executive in wartime thus satisfied the requirements of the War Powers Act of 1973. Former CIA Inspector General L. Britt Snider argues that the AUMF is far too vague, and open for expansion and interpretation, for consideration as an act of war.<sup>44</sup> Legal counsel within the Pentagon, however, argue that the AUMF is nothing more than an expression of legal, inherent right of self-defense.<sup>45</sup>

The debate over the legality and purview of the AUMF is not an academic or theoretical one. How one interprets the AUMF has a significant impact in any analysis of Title 10 and Title 50 authorities as well as Congressional oversight. If one accepts Snider's interpretation, then the AUMF falls short of a declaration of war and therefore all missions conducted under it which hide the sponsor are covert action, subject to Title 50 authorization and Congressional notification.<sup>46</sup> The other side of the debate, championed by former Under Secretary of Defense for Intelligence (USD[I]) Stephen Cambone, suggests that as the AUMF is a declaration of war, and all military actions within the theater of war should be considered as Traditional Military Activity authorized under Title 10 with no form of Congressional oversight.<sup>47</sup>

Between these two polar opposite interpretations there is considerable room for debate. Any workable way forward must involve a degree of compromise between them. The AUMF, which suited US purposes for counterterrorism against a nebulous and elusive global

---

<sup>43</sup> Eric Rosenbach and Aki J. Peritz, *Trials by Fire, Counterterrorism and the Law* (Cambridge: Belfer Center for Science and International Affairs, 2010), 8.

<sup>44</sup> Kibbe, "The Rise of the Shadow Warriors," 109.

<sup>45</sup> Michael McAndrew, "Wrangling in the Shadows: The Use of United States Special Forces in Covert Military Operations in the War on Terror," *Boston College International and Comparative Law Review* 29, no. 1 (1 December 2006).

<sup>46</sup> Kibbe, "The Rise of the Shadow Warriors," 109.

<sup>47</sup> "Congress to Restrict the Use of Special Ops," *The Washington Times*, 13 August 2003, <http://www.washingtontimes.com/news/2003/aug/13/20030813-120409-8659r/?page=all>.

network of terrorism, is over a decade old. Despite this fact, however, there has been adequate opportunity for it to be challenged legally or politically on the grounds that it is too comprehensive and open to interpretation. So far no individual or organization has sought to constrict the authorities associated with the AUMF or amend it. Some members of Congress did challenge Secretary Cambone's interpretation on and has since clarified its position on subject of TMA. The real question is what will happen if Congress goes beyond amendment and repeals AUMF in the near future, particularly after the death of Osama bin Laden and the perception that al-Qaeda is broken and shattered.

### **Risks Both Domestic and International**

There are inherent risks in any action but covert and clandestine actions carry even more. The risks are not exclusively borne by the operators but also shared by the authorizing authority as well as the mission's commander. Considerations of risk should be a major factor in deciding to execute covert or clandestine missions.

A 2009 Gallop poll discovered 82 percent of Americans have a "great deal" or "quite a lot" of respect for the military.<sup>48</sup> The CIA has not enjoyed the same level of support over time. This level of trust permits the military to avoid the level of scrutiny for its clandestine activities that Congress gives to almost every significant covert action conducted by the CIA.

CIA covert action is monitored in two Congressional committees, one in each the House and Senate. The executive branch informs these committees of programs prior to their commencement but Congress has little say in whether they occur or not. Rep Hank Johnson said, "we have budgetary control...but no restriction."<sup>49</sup> When the military

---

<sup>48</sup> Lydia Saad, "Congress Ranks Last in Confidence in Institutions," Gallup Politics, <http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx> (accessed 19 March 2012).

<sup>49</sup> Kimberly Dozier, "Officers: No Plans for CIA to Run War," *Philadelphia Inquirer*, 8 March 2012, 6.

executes its covert action missions the process is even more cumbersome and provides fewer restrictions. Congress bases their oversight on the organization; however, Title 10 and Title 50, which grant the authorities, are not. This makes for a very confusing notification process within Congress that erodes the ability to conduct effective oversight.

The legal definitions of covert, clandestine, and TMA are either unclear or unwieldy as discussed in Chapter 1. In 2003 a DoD memo leaked to the press tried to clarify the distinctions, by explaining that the military conducts clandestine operations where the CIA conducts covert ones.<sup>50</sup> This simplistic separation between the two misconstrues a much more subtle, nuanced distinction. Nothing legally prevents organizations other than the CIA from conducting covert action. However, only the President has the power to authorize all covert actions legally through the process of signing a “finding.”<sup>51</sup> By the executive branch simply labeling an action as “covert,” it triggers a series of steps including Congressional notification and legal review. Simply defining all military action as clandestine precludes these oversight actions or review as Congress has not defined the term or its oversight requirements.

Legally risks are one thing but operational risks overseas are for the personnel conducting covert actions is something entirely different. If US military members participate in covert action they could forfeiting their legal rights under the Geneva Convention.<sup>52</sup> To receive prisoner of war status a military member must be under the command of someone responsible, wear distinctive marking (such as a uniform), carry arms openly and conduct themselves in accordance with laws and customs of war.<sup>53</sup> Even though military special operators have relaxed uniform

---

<sup>50</sup> “Congress to Restrict the Use of Special Ops,” *The Washington Times* (13 August 2003)

<sup>51</sup> 50 U.S.C. § 413(b)

<sup>52</sup> Kibbe, “The Rise of the Shadow Warriors,” 113.

<sup>53</sup> International Committee of the Red Cross, “Convention (III) relative to the Treatment of Prisoners of War, 12 August 1949,” Part I, Art 4 (2),

standards, they wear a legally-defensible uniform nonetheless and should receive guaranteed protections.<sup>54</sup> When those same operators participate in covert actions, and try by definition to hide that they are US government employees, they may forgo their legal rights and a government might consider them as unlawful combatants guaranteed no rights and privileges.<sup>55</sup> CIA paramilitary personnel operate willingly and freely with this knowledge and accept these risks personally. Military personnel conducting covert action may not be as familiar with the traps and pitfalls of their legal status or the position of risk in which they are placing themselves.

The last area of risk in covert action for the U.S. is in the realm of international law. Under the Law of Armed Conflict the military is bound to act in accordance with customary international law, treaties, and international agreements concerning armed conflict.<sup>56</sup> By conducting its military operations in accordance with LOAC the U.S. upholds the rule of law internationally. States tacitly accept that espionage is part and parcel of statecraft and some abide by certain informal agreements should their personnel be captured. Even bitter adversaries such as the U.S. and the Soviet Union rarely executed each other's covert agents; more often, captured agents were interrogated for information and after a period of time were exchanged for their own agents captured by the enemy. The U.S. has gone one step beyond tacit agreement and overtly and explicitly authorizes CIA personnel to break international law while conducting covert action in EO 12333.<sup>57</sup> The President could authorize military covert actions under this same exception but military personnel

---

<http://icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e63bb/6fef854a3517b75ac125641e004a9e68> (accessed on 24 May 2012).

<sup>54</sup> William H. Ferrell, III, "No Shirt, No Shoes, No Status: Uniforms, Distinction, and Special Operations in International Armed Conflict," *Military Law Review* 178, (Uniforms, Distinctions, and Status, 2003), 137.

<sup>55</sup> W. Hays Parks, "Special Forces' Wear of Non-Standard Uniforms," *Chicago Journal of International Law* 4, no. 2, (Fall 2003), 511-513.

<sup>56</sup> McAndrew

<sup>57</sup> EO 12333 United States Intelligence Activities.

found operating in this way by another government may be in a precarious, if not unpleasant (torture) or lethal (executed) position if they are compromised.

### **Conclusion**

The relationship between DoD and CIA overt, covert, and clandestine counterterrorism operators currently is the epitome of interagency cooperation and collaboration. The basic authorities under which they operate reside in two different titles of the U.S. Code. Title 10 deals mainly with DoD military operations and forces while Title 50 provides specific authorizations for the intelligence community. To most outside observers the line between these titles and their authorities is distinct. However, as this chapter has made clear, the language within Title 50 does not preclude the military from participating in covert action. The line between Title 10 and Title 50 should be a distinct one if only to protect the personal safety of those executing missions under their authority. As this chapter has made clear, the similarities between covert and clandestine activities mean that policy and decision makers can and have manipulated both terms to their operational advantage.

The debate regarding covert and clandestine operations centers on the organization in charge, or command, of a specific operation. If the CIA is the lead agency then the President must authorize the covert action personally under the stipulation of Title 50 even if DoD forces carry out the mission as was the case in Operation NEPTUNE'S SPEAR. In addition, the executive branch must notify Congress of the operation prior to its conduct. If DoD is in charge of the activity then the CIA may provide specialist personnel and capabilities but the operation itself may be covert or clandestine depending on who authorized it. The overall mission commander, within a COCOM, as well as the degree of deniability desired for the DoD operation, determines how and under what circumstance the President authorizes the operation. Regardless of

how this authorization works, Congressional oversight may be side-stepped or avoided altogether. A lack of oversight of “secret” activities not only may be illegal but once their details are revealed, often after a spectacular failure or compromise, the result is often Congressional scrutiny, highly restrictive oversight mechanisms, and the reduction of operational flexibility to conduct covert and clandestine missions.



## CHAPTER 3

### CYBERCOM AND THE NSA: Two Bodies, One Head

*So what does the definition between covert and clandestine look like in law? They're very difficult. It's very difficult to understand this.*

General Cartwright, former VCJCS in interview about cyber

The DoD declared cyberspace the newest warfighting domain alongside the other domains of land, sea, air, and space.<sup>1</sup> Unlike the SOCOM and CIA relationship discussed in Chapter 2, the cyber “relationship” between the National Security Agency (NSA) and CYBERCOM is a relatively new marriage of intelligence gathering and military capability. This relationship, solidified in a common leader, and sealed in layers of secrecy and compartmentalization, represents a new model for partnership and authority sharing. This partnership, however, creates problems for laws designed with distinct organizational lines, and in particular for oversight of cyber activities, as this chapter demonstrates.

#### CYBERCOM and the NSA

In 1952 President Truman established the NSA and made it a part of the Defense Department to enshrine the decisive codebreaking expertise obtained during World War II.<sup>2</sup> Today the NSA is a member of the Defense Intelligence Community and is responsible for signals intelligence, information assurance, and enabling network warfare.<sup>3</sup> The NSA kept pace with the rapid developments that were part of the communication revolution, such as satellite, cellular, and fiber optic

---

<sup>1</sup> William J. Lynn, III, US Deputy Secretary of Defense, (address, Defense Information Technology Acquisition Summit, Washington, D.C., 12 November 2009).

<sup>2</sup> National Security Agency/Central Security Service, “NSA/CSS Frequently Asked Questions,” [http://www.nsa.gov/about/faqs/about\\_nsa.shtml](http://www.nsa.gov/about/faqs/about_nsa.shtml) (accessed 21 April 2012).

<sup>3</sup> Dana Priest and William Arkin, *Top Secret America*, (New York: Little, Brown and Company, 2011), 5.

methods of transmission, and the Agency developed an incredible cyber capability. Already by 1996 NSA had the capability through its worldwide network of intercept stations to monitor Inmarsat calls. They tracked the phone number Osama bin Laden used, listening to his phone calls and orders without his knowledge.<sup>4</sup> Given that the NSA is part of the intelligence community, Title 50 of the US Code governs their actions, thereby limiting the NSA's ability to take action without a signed, classified Presidential Finding.

The call within national security circles to establish a new organization within the military to handle cyber matters was on the table for some time. Leaders in the Pentagon and elsewhere around the National Capital Region were convinced of the necessity but were still stinging from the premature rise, and precipitous fall, of Space Command.<sup>5</sup> They also knew cyber expertise already existed in the National Security Agency and did not want to duplicate this expensive, mature capability.<sup>6</sup> There was some discussion of simply making the NSA the new lead for cyber issues but this did not bridge the complex legislative landscape between Title 10 and Title 50. The DoD, in the eyes of senior leaders, required a new organization responsible for this new domain.

CYBERCOM became operational May 21, 2010 under the leadership of General Keith Alexander (USA).<sup>7</sup> He was already the Director of the NSA when CYBERCOM stood up. As part of a compromise between those who desired a separate command and those wanting the NSA in the lead for cyber issues, the Secretary of Defense and the Senate gave General Alexander command of both and a fourth

---

<sup>4</sup> James Bamford, *Body of Secrets*, (New York: Anchor Books, 2002), 617-618.

<sup>5</sup> Priest and Arkin, xv.

<sup>6</sup> Richard Clarke and Robert Knake, *Cyber War*, (New York: HarperCollins, 2010), 38.

<sup>7</sup> US Strategic Command, "CYBERCOM Fact Sheet," <http://www.stratcom.mil/factsheets/Cyber-Command>, (accessed 3 May 2012).

star required for the command.<sup>8</sup> Within the DoD this command relationship is informally known as “dual-hatting” which allows for a single commander to be in charge of two organizations. This chapter discusses the strengths and weaknesses of dual-hatting in a subsequent section.

CYBERCOM is a sub-unified command under US Strategic Command (STRATCOM). As a functional combatant command, STRATCOM, and therefore CYBERCOM, have global responsibilities. These elements—a dual-hatted command and a global purview under a unified command—gives CYBERCOM its Title 10 authorities to wage “cyber war” and deliver cyber effects to the battlefield.

### **Title 10/50 authorizations for cyberspace**

When examining cyber it is helpful to use the means it employs as a primary focus for its evaluation. The means within cyberspace are inherently clandestine in nature. Much of what the press labels as attacks are actually examples of cyber espionage. The problem with the espionage label though is governments generally accept that countries spy on each other, but do we attack those countries? No, because we are collecting on them at the same time.<sup>9</sup> The government keeps offensive operations designed to generate an effect highly classified; concealing the actor is possible in cyberspace because the problem of attribution determination.<sup>10</sup> Some would argue the means are actually covert since there is usually intent to disguise or hide the actor in cyberspace but the discussion in the Introduction and Chapter One demonstrated the narrow definition of covert is best suited to explaining policy decisions and not the acts themselves. As the former Vice-Chairman of the Joint Chiefs of Staff, General James Cartwright, said in an interview with the

---

<sup>8</sup> Clarke, 39.

<sup>9</sup> Chris Bronk, “Treasure Trove or Trouble: Cyber-Enabled Intelligence and International Politics” *American Intelligence Journal* 28, no. 2, (2010): 28-29.

<sup>10</sup> Bronk, 28.

Armed Force Information Service: “When you enter cyber, do we put the tailflash on every one of the dots and digits that says ‘United States Air Force has passed through here?’ Probably not.”<sup>11</sup> This quotation illustrates that the problem of attribution is just as difficult for our adversaries as it is for us (or other potential users).

The current cyber organization, CYBERCOM, rests on a delicate balance of authorizations between the Title 10 and Title 50 of the US Code. The relationship between these authorizations is perilous at best or blurry at worst. Table 2 puts this balance in graphical form and provides a framework for better understanding, through examination of the individual characteristics, how CYBERCOM and the NSA straddle the overt, covert, and clandestine authorities divide. For this discussion the developer and authority to execute overt, covert, and clandestine missions remains constant across the cyberspace example. When viewed from the perspective of cyber domains and authorities, however, the other attributes of the framework help explain the subtle but important differences from the paramilitary examples outlined in Chapter 2.

---

<sup>11</sup> Jim Garamone, “Questions Abound in Cyber Theater of Operations, Vice Chairman Says,” *Armed Forces Information Service*, 9 June 2009.

**Table 3: Characteristics (Cyber)**

	<b>Covert Action</b>	<b>Clandestine Activity</b>	<b>Traditional Military Activity</b>
<b>Developer</b>	NSC	Military/Agency Director	Military/Agency Director
<b>Execute Authority</b>	President	SecDef/COCOM <sup>1</sup>	SecDef/COCOM <sup>1</sup>
<b>Oversight</b>	Intelligence Committee	Armed Services/ Other	Armed Services
<b>Legal Authority</b>	Title 50/ EO 12333	Title 10/50 EO12333	Title 10
<b>Deniability</b>	Sponsor	Act	None
<b>Policy Basis</b>	CIA	Agency	Military
<b>Command</b>	CIA	Military/Agency Director <sup>2</sup>	Military

<sup>1</sup> President or SecDef must approve SOCOM missions (PL 108-136)

<sup>2</sup> Agency directors may supervise their own missions if they are conducting clandestine operations.

*Source: Author's Original Work*

### **Deniability**

One of the defining characteristics of covert action is deniability. Covert action conceals the sponsor of the act taking place and clandestine activities hide the act itself and sometimes delay acknowledgement of the sponsor. However, in Traditional Military Activity (TMA) the military conceals neither the sponsor nor the act. Since the means employed by CYBERCOM and the NSA are secretive they are unable to shed their “cloak and dagger” quality making it difficult to understand how cyber operations can ever be transparent enough to be classified as TMA.

When the NSA and CYBERCOM conduct certain operations they are able to use other exceptions to the covert action definition: intelligence collection and routine support to overt activities. Intelligence

collection is in the mission statement for the NSA so it stands to reason they would characterize most of their cyber means in this category. CYBERCOM, in contrast, uses the routine support to overt activities exception. Currently as a sub-unified command CYBERCOM's support to other combatant commanders would qualify under this exception. If they act independently in defense of the nation as proposed, then routine support to overt activities may not apply any longer, requiring them to use a revised definition of TMA.

### **CYBER and TMA**

CYBERCOM, since its inception, has fought valiantly to define what TMA means to the organization. In the 2012 National Defense Authorization Act Congress sought to clarify this definition for the Command. The House of Representatives included a more stringent definition of TMA within their bill specifically for CYBERCOM. The Senate, however, did not agree with the definition or language provided by the House. The first attempt at clarifying TMA for cyber did not survive the conference committee for the bill. In the Conference Report, however, the Members from both houses agreed to include the following text, "The conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes traditional military activities in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities."<sup>12</sup> This enhanced, cyber definition for TMA is crucial to how the DoD views cyber capabilities.

Policy makers divided up defense of the cyberspace domain between the DoD (.mil domain) and the Department of Homeland Security (DHS; .gov domain) while the private sector is responsible for securing and policing, to the extent possible, its own areas (.com, .edu,

---

<sup>12</sup> House Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2012*, 112th Cong., 1st sess., 2011, HR 112-329-Part 1.

and .org domains). DoD and DHS signed a memorandum of agreement in 2010 to ensure cooperation and collaboration between both agencies.<sup>13</sup> However, CYBERCOM has lobbied Congress for the ability to defend cyberspace much in the same way the DoD defends the airspace of the United States. In doing so, the CYBERCOM commander has asked the Chairman of the Joint Chiefs of Staff to change the Standing Rules of Engagement (SROE) to reflect the evolving character of the cyber threat. A subsequent section tackles the SROE specifically. The analogy that CYBERCOM uses to frame the argument to change the SROE is the subject of the next section.

### **The Inbound Missile Analogy**

In support of their argument CYBERCOM has drawn on a particularly appealing analogy. The rationale behind this analogy is that the effects of a cyber attack may be instantaneous and potentially devastating to the country. In CYBERCOM's eyes there is a perceived need for an expedient, pre-canned response to deal with this threat.<sup>14</sup> In both CYBERCOM and Congress advocates have drawn parallels between an impending cyber attack and responding to a missile attack on the homeland. They posit that if an inbound missile were to appear suddenly on warning sensors protecting the US there is a predetermined, pre-coordinated, immediate response not requiring further policy maker decisions. With cyber there is no such response currently, hence the need for expanded authorities.

Oxford University professor Yuen Foong Khong penned one of the most influential books on decision making using analogies. In his book, Khong uses a six-part formula for evaluating or creating an analogy, the

---

<sup>13</sup> Secretary of Defense and Secretary of Homeland Security, Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity, 27 September 2010.

<sup>14</sup> House Armed Services Subcommittee on Emerging Threats and Capabilities, *Proposed Fiscal 2013 Defense Authorization as it Relates to Information Technology and Cyber Operations*, 112th Cong., 2nd sess., 20 March 2012.

first three parts of his formula are most useful in this example as they pertain to illuminating an ill-defined problem. The final half of his analogy construct deals with evaluating the implied policy solution and alternative answers.<sup>15</sup> He says first the analogy must define the nature of the problem to allow a policy maker to make a direct reference to a problem with which they are accustomed.<sup>16</sup> In this example Congress already has a frame of reference regarding the problem of inbound missiles, particularly given the political decisions regarding missile defense in this country over the past decade. Recently there has been discussion about the deployment of interceptor missiles along the coast as a point defense as an indication of the depth of Congress' involvement and understanding of the subject.<sup>17</sup>

Second, Khong points out the analogy should give a policy maker a sense of the stakes involved in the problem.<sup>18</sup> The intended implication of the inbound missile analogy is that imminent destruction will occur if there is no timely defensive counter or reaction. The subtle implication being the analogy, however, is that like an inbound missile an incoming cyber attack will have an easily determined point of origin and a method of defending or responding. Many authors discuss the problem of attribution in the unclassified literature on cyber. In addition to highlighting the attribution problem regarding cyber attacks in general, Mark Bowden wrote how difficult it was to dissect, block, and then disinfect computers afflicted with the Confiker worm.<sup>19</sup> Inbound cyber attacks may not prove to be any easier to identify the source, attribute intent, and respond in kind.

---

<sup>15</sup> Yuen Foong Khong, *Analogies at War*, (Princeton: Princeton University Press, 1992), 20-21.

<sup>16</sup> Khong, 20.

<sup>17</sup> Associated Press, "House Panel Votes to Build Missile Defense Site on East Coast Despite Pentagon Disapproval," *The Washington Post*, 9 May 2012 <http://www.washingtonpost.com/world/national-security/republican-led-house-panel-considers-bill.html>.

<sup>18</sup> Khong, 20.

<sup>19</sup> Mark Bowden, *Worm*, (New York: Atlantic Monthly Press, 2011). Bowden describes the months and man-hours behind unraveling the Confiker worm which worked its way around the world creating an extremely large botnet.

Third, according to Khong, an analogy should suggest a solution to the problem identified.<sup>20</sup> To CYBERCOM the solution to inbound cyber attacks is the same as the inbound missile. This solution is amending the Standing Rules of Engagement (SROE) to include a cyber annex to delegate authorities of response down to military commanders. The analogy of the inbound missile leads one logically to this conclusion but as Khong points out in the later chapters of his book, in order for an analogy to be effective it must also be correct. The next section explains what the SROE is in addition to providing an assessment of the correctness of the analogy.

### **SROE**

The SROE exist to “implement the inherent right of self-defense and provide guidance for the application of force for mission accomplishment” according to the unclassified 15 January 2000 iteration.<sup>21</sup> The idea behind the SROE is to establish expedient solutions to pre-determined problems to ease and speed decision making and response execution during times of crisis. Paul Walker concludes in his monograph that the exceptions to covert action provided in the TMA language produces a “bright line test” to allow the military freedom of action to operate in cyberspace in this situation.<sup>22</sup> He further argues the military stewardship exemplified in war plans and rules of engagement have justified Congress in providing this exception.<sup>23</sup> Walker is attempting to argue the pace of operations in cyberspace is such that traditional means of covert action approval are too slow and will be ineffective in cyberspace. CYBERCOM makes a similar argument while

---

<sup>20</sup> Khong, 21.

<sup>21</sup> Federation of American Scientists, “CJCS Instruction 3121.01A, 15 January 2000,” [http://fas.org/man/dod-101/dod/docs/cjcs\\_sroe.pdf](http://fas.org/man/dod-101/dod/docs/cjcs_sroe.pdf).

<sup>22</sup> Paul Walker, “Traditional Military Activities in Cyberspace: Preparing for ‘Netwar’” *Selected Works* May 2010, 30, [http://works.bepress.com/paul\\_walker/2](http://works.bepress.com/paul_walker/2) accessed 23 May 2012.

<sup>23</sup> Walker, “Traditional Military Activities in Cyberspace: Preparing for ‘Netwar.’”

attempting to amend the SROE to allow field commanders the authority to use cyber weapons in the event they detect an incoming attack.

The debate around the SROE for cyber though goes deeper than the argument for expedience. CYBERCOM is a sub-unified command and does not have a geographic area of responsibility. Much in the same way the CYBERCOM commander has responsibilities to the NSA, the Command also cannot act globally without impinging on other geographic combatant commanders under the current Unified Command Plan organization.<sup>24</sup> Allowing the CYBERCOM Commander to operate unilaterally upon seeing what appears to be an incoming attack would be like using an airplane to bomb another country without telling the responsible geographic combatant commander.<sup>25</sup>

Even more problematic than geographic responsibilities is a lack of precision regarding some aspects of cyber, including what should be included and excluded in its definition. Furthermore there is no clear definition of what constitutes an attack in cyberspace which imperils the analogy equating cyber attacks with an in-bound missile attack.<sup>26</sup> Despite these challenges CYBERCOM has advocated for broad authorities to take action within the United States across cyber domains currently assigned to other agencies or individuals without establishing a common attack definition.<sup>27</sup> General Alexander argued “in order to stop it [a cyber attack], you have to see it in real time, and you have to have those authorities.”<sup>28</sup> The implication of his conclusion is absolutely clear. CYBERCOM will require expanded authorities in order to deal with imminent surprise attacks in the future. As General Alexander said

---

<sup>24</sup> Wesley R. Andruess, “What U.S. Cyber Command Must Do,” *Joint Forces Quarterly* 59, 4th Quarter 2010, 119.

<sup>25</sup> CYBERCOM uses an inbound missile analogy in much of their congressional dealings so the bomber analogy while clunky works.

<sup>26</sup> Cheryl Pellerin, “Cyber Operations Give Leaders New Options, Official Says,” *American Forces Press Service*, 12 April 2012.

<sup>27</sup> Ellen Nakashima, “When Is a Cyberattack a Matter of Defense?” *The Washington Post*, 27 February 2012.

<sup>28</sup> Ellen Nakashima, “NSA Thwarted in Cybersecurity Initiative,” *The Washington Post*, 28 February 2012.

in a different interview, “What I’m pushing for is to have those [authorities in the rules of engagement] so that we can protect and prevent” as well as respond.<sup>29</sup> Without a clear understanding of what an attack is, a definitive determination of its origin, the ability to guarantee precision in re-attack, or clear legal authorities even within the US changing the SROE is dangerous.

### **Legal Authority**

While the line between covert action and clandestine activities has at times been blurry depending on your vantage point, actions authorized under TMA have attempted to stay clear of both and be as transparent as possible. The primary challenge related to CYBERCOM is that its authorities span them both. For example, activities directed by the NSA fall under intelligence gathering provisions and covert action of US Code, both of which are found in Title 50. CYBERCOM itself, however, operates as a sub-unified command with military authorities found in Title 10.

The result of this marriage of intelligence gathering in the NSA and operations in CYBERCOM is power and command residing in one person whose authorities straddles two distinct and almost mutually exclusive statutes. The conglomeration of roles and responsibilities has the potential to hobble the effectiveness of both organizations unless they complement each other mission sets.<sup>30</sup> Since these organizations share a single commander it also means this individual must report to both the intelligence and armed services committees of both houses of Congress. The challenge within a democracy, and particularly the American experiment with this form of government, is that it raises the possibility of one person exploiting the division of authorities as the next section makes clear.

---

<sup>29</sup> Shaun Waterman, “Cyber Warfare Rules Still Being Written,” *The Washington Times*, (20 March 2012).

<sup>30</sup> Wesley R. Andruess, “What U.S. Cyber Command Must Do,” 116.

### **Dual hatting**

The way in which CYBERCOM and the NSA have navigated the treacherous waters between Title 10 and Title 50 authorities is by naming one leader to head both organizations simultaneously, known as dual-hatting. Dual-hatting is not a new phenomena and it has occurred in other military organizations in the past. For example, US Transportation Command and the USAF Air Mobility Command had a single commander until recent years, which allowed one voice to speak on global air mobility issues. The idea behind dual-hatting is to allow a single individual to head similar organizations to gain efficiencies within the system by reducing overlapping capabilities or staff structures, speed the response of decision making, and prevent potential friction and misunderstanding between organizations charged with the similar tasks. What makes this dual-hatting arrangement work is that both functions are not only clearly related but they operate within a single, overt set of authorities in Title 10.

The arguments in support of dual-hatting for cyber are obvious and functional in nature. First, the NSA and CYBERCOM both operate in cyber domain and have global responsibilities. Second, the NSA has a more mature cyber capability than CYBERCOM based on years of experience. Third, there is extensive technological overlap between the primary function of NSA, signals collection, and the primary function of CYBERCOM, cyber warfare.<sup>31</sup> Finally, a single commander can eliminate traditional budgetary infighting between the two similar organizations.

Although dual-hatting for cyber appears to rely on sound reasoning, logic and seems to be a panacea to resolve many functional and organizational issues related to cyber; the problems it creates regarding oversight and authorities are significant. From a policy perspective dual-hatting creates tensions within the system of checks

---

<sup>31</sup> Paul R. Pillar, "Unintelligent Design," *The National Interest* 109, Sep/Oct 2010, 47.

and balances. Congress created Titles 10 and 50 to ensure that intelligence collection and military operations are as separate and distinct as possible. As Chapter 4 suggests, even distinct separation is under siege given changes within the military and intelligence communities since 11 September 2001. Dual-hatting the commander of CYBERCOM as the Director of the NSA focuses these authorities under one individual. This dual-hatting arrangement raises questions about the potential militarization of cyberspace which the Deputy Secretary of Defense, William Lynn III, took great pains to deny publically in an article in *Foreign Affairs*.<sup>32</sup>

The CYBERCOM dual-hatting arrangement contains an internal challenge. This arrangement “ignores the fundamental point that someone wearing two hats has a balancing act in identity and status that usually leaves one of the roles either falling by the wayside or hidden under the other.”<sup>33</sup> Peter W. Singer, a Senior Fellow at the Brookings Institution in Washington, conducted interviews with military cyber personnel on the subject of dual-hatting authorities. Singer found that they described themselves as carrying out Title 10 and Title 50 roles at any given moment depending on the task.<sup>34</sup> Their description is disturbing for a number of reasons. Congress created these titles in US Code separately to keep organizations from overstepping their intended purpose. On a purely administrative level, combining both Title 10 and 50 functions under a single commander offers the potential one will get short shrift. General Michael Hayden offers a unique perspective on this subject. During and immediately following 11 September, Hayden was director of the NSA. Subsequent to that job he served as director of the CIA. On the subject of dual-hatting between Title 10 and 50 functions,

---

<sup>32</sup> William J. Lynn, III, US Deputy Secretary of Defense, (address, Defense Information Technology Acquisition Summit, Washington, D.C., 12 November 2009).

<sup>33</sup> P.W. Singer, “Essay: Double-Hatting Around the Law,” *Armed Forces Journal*, June 2010, <http://www.armedforcesjournal.com/2010/06/4605658/>.

<sup>34</sup> Singer.

Hayden concluded that, “They’re both more than full-time jobs. Frankly, having the director of one of the nation’s premier intelligence agencies also serve as a combatant commander creates a conflict of interest.”<sup>35</sup> Hayden understates his conclusion. This construct not only has the potential to create a conflict of interest but it also makes it extremely difficult for one person to have visibility on all activities of both agencies. The implications of this are clear: subordinates could conduct potentially illegal activities without a commander knowing, but more troublesome for a democracy is the potential for one individual to willingly or unwillingly mislead or misrepresent the activities of two very powerful agencies to the two separate Congressional committees charged with their oversight in the name of national security. Although perhaps remote, the history of covert action in the United States suggests that this is a very real possibility when power is concentrated too much in individuals or single organizations without sufficient transparency or oversight.

### **Conclusion**

Peter Singer reached the conclusion in his article that “Titles 10 and 50 were meant to be something different, and that difference remains very important both politically and legally.”<sup>36</sup> CYBERCOM and the NSA are complimentary agencies that should share information and personnel when appropriate. However, the current dual-hatting command construct places these agencies too close together for it to be healthy for either.

In the context of the framework for analysis outlined in Chapter 1, it is clear that CYBERCOM’s dual-hatted command relationship is fundamentally flawed. The analysis in this chapter makes evident Congress never intended for one person to wield so much power on either

---

<sup>35</sup> Ellen Nakashima, “Military Leaders Seek Higher Profile For Pentagon’s Cyber Command Unit,” *The Washington Post*, 1 May 2012.

<sup>36</sup> Singer.

side of the Title 10/50 divide, much less combine them together. The separation ensures the Madisonian checks and balances underpinning our system, which gives it its strength and resilience, remain in place. Combining the two titles in one organization or person offers an avenue for overreach or expansion of authorities that is potentially detrimental to the long-term health and viability of the Republic.



## **CHAPTER 4**

### **POLICY CONSIDERATIONS SINCE 9/11**

*War will not be waged by armies but by groups whom today we call terrorists, guerrillas, bandits and robbers, but who will undoubtedly hit on more formal titles to describe themselves.*

Martin van Creveld, *The Transformation of War*

Congress divided authorities for overt, covert, and clandestine action between Title 10 and Title 50 in 1947 but until recently the overlap between them has not been much of a policy or legislative issue.<sup>1</sup> As previous chapters have noted, since 1947 the meaningful issue has been the struggle between the executive and legislative branches of government over freedom of action and interpretation of the letter versus the spirit of the law. Since 11 September 2001, however, changes in the strategic environment have illuminated and exacerbated fissures in this division of authorities. The threat posed by transnational terrorism, the information age, and the dramatic growth in capability of the non-state actor brought on changes as this chapter suggests. Organizations and agencies working on behalf of the President, Congress, and the American people have struggled to keep pace with the changing and elusive nature of contemporary threats. They have sought to do so by exploiting any advantage, technical or legislative, to deal with the threat posed by non-state actors. In seeking advantages and exploiting legal loopholes U.S. national security organizations and agencies have further blurred the intended division between Title 10 and 50. In addition, these organizations and agencies challenge the traditional oversight mechanisms put in place around rigid lines of authority. This chapter reviews changes in the security environment, describes how oversight

---

<sup>1</sup> *National Security Act of 1947*, Public Law 80-253, 80th Cong., 1st sess. (26 July 1947).

has barely evolved in the process, and suggests future challenges to oversight over overt, covert, and clandestine operations.

### **Strategic Environment Today**

The past decade has seen the rise of what some analysts have labeled the “strategic person.” A strategic person is a single actor (cells, groups, or grassroots organizations) or individual, operating with or without state sponsorship, which perpetuates political acts, including violence, against nation states in order to provoke a response. National governments today increasingly feel the pressure from, and focus on combating, such empowered non-state actors. Nation-states perceive these individuals and groups as a grave threat to national security, for reasons which shall become clear below, and in the process catapult nefarious groups individuals into infamy.

Individuals who have a grievance against the state, and seek the means to humiliate or coerce national leaders, can be a potent threat today. In the past, such individuals could conduct acts of sabotage, subversion, or terrorism but the effectiveness of their actions was often limited locally. For example, the series of anarchist-inspired bombings in the United States from 1919-1920, or sabotage against American port facilities and infrastructure during the two world wars, were both limited in scope, scale, and impact for a number of social and technical reasons.<sup>2</sup> Today these attacks barely register in the national consciousness. The combination of technical means readily available commercially to individuals has changed the impact they can have. Working either alone or networked to others they produce effects once

---

<sup>2</sup> For details of the so-called “Red Scare” bombings, which included attacks against the U.S. Attorney General and targets on Wall Street, see Charles H. McCormick, *Hopeless Cases: The Hunt for the Red Scare Terrorist Bombers* (Lanham, MD: University Press of America, 2005), On Imperial German attacks against the United States in New Jersey during the First World War, see Jules Whitcover, *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914-1917* (Chapel Hill, NC: Algonquin Books, 1989). On attacks against targets in New York state and city by Nazi German saboteurs and agents during the Second World War as part of the ill-fated “Operation Pastorius,” see Michael Dobbs, *Saboteurs: The Nazi Raid On America* (New York: Random House, 2004).

only envisioned for states. As discussed in the previous chapter, for example, cyber warriors focus on protecting against those seeking to wreak havoc on infrastructure already hardened against more traditional terrorist attacks. The so-called “hacktivist” threat is very real and increasingly diverting time, money, and energy away from traditional state-on-state defense. The following paragraphs outline just how strategic individuals and groups today can be.

Individuals today possess unprecedented access to information and the ability to disseminate it to a wide audience using information technologies. In 2010, US Army Specialist Bradley Manning allegedly released 150,000 classified diplomatic cables, 90,000 classified documents, and video of an American helicopter attack in Afghanistan.<sup>3</sup> A single disgruntled junior enlisted soldier managed to not only download this data, and carry it away on his person, but also to have it published. The Manning case not only calls into question the ability of U.S. government organizations to secure information, and therefore challenge its credibility, but the release of the information damaged American diplomacy by revealing embarrassing details and exchanges about and with nations that are the staple of international diplomacy. Manning did not complete his actions alone. Using other forms of information technology, he sought out and negotiated with members of the Wikileaks website to have the information he obtained illicitly posted on the Internet for all to see.<sup>4</sup>

Individuals, particularly those with inside access and information, are only one illustration of how strategic actors operate today. Other individuals and groups have managed to use technological means to compromise “secure” means of transmitting information and data. In January 2012, members of the group Anonymous hacked into a secure

---

<sup>3</sup> Elisabeth Bumiller, “Army Broadens Inquiry into Wikileaks Disclosure,” *New York Times*, 30 July 2010, A1.

<sup>4</sup> Bumiller, A1.

teleconference between agents of Scotland Yard and the FBI and recorded the conversations they were having about the group.<sup>5</sup> A month later, Anonymous published their recording which discussed the threat posed by the group as well as law enforcement initiatives designed to apprehend hacking suspects.<sup>6</sup> Members of Anonymous were able, but luck or design, not only to hack into costly encrypted and secure communications means at right time but also reveal embarrassing information to the public and the international community. Nation-states with vast budgets, personnel, and infrastructure to fund high-technology projects could intercept, decrypt, and analyze this type of information through agencies such as the National Security Agency and the Government Communications Headquarters (GCHQ). Such capabilities are increasingly available to almost anyone with a computer, Internet access, moderate skill, and time.

Technologies available to individuals and groups possess potential for purposes beyond humiliating a state or revealing classified or sensitive information. They can use such technologies to improve the precision and lethality of the violence they carry out for political purposes. One capability groups and individuals can acquire with an Internet connection are surveillance and imagery means. In 2007 Iraqi insurgents apprehended by coalition forces had Google Earth images of some British military bases in Iraq to aid in the planning for their attacks.<sup>7</sup> Google Earth publishes commercially-available one-meter resolution satellite images photographs for many locations, or five-meter resolution for most other areas.<sup>8</sup> Seeking to downplay the discovery,

---

<sup>5</sup> "Anonymous Gain Access to FBI and Scotland Yard Hacking Call," *BBC News*, 3 February 2012, <http://www.bbc.co.uk/news/world-us-canada-16875921?print=true> (accessed 20 May 2012).

<sup>6</sup> "Anonymous Gain Access to FBI and Scotland Yard Hacking Call," *BBC News*, 3 February 2012.

<sup>7</sup> Kelly Hearn, "Terrorist Use of Google Earth Raises Security Fears," *National Geographic News*, 12 March 2007, <http://news.nationalgeographic.com/news/pf/93861668.html> (accessed 20 May 2012).

<sup>8</sup> Google, "Google Earth Frequently Asked Questions," Google, <http://support.google.com/earth/bin/answer.py?hl=en&answer=187961&topic=2376010&ctx=topic> (accessed 20 May 2012).

some DoD leaders argued in 2007 that even though terrorists and insurgents had access to Google Earth imagery, they had yet to use it in an attack.<sup>9</sup>

The following year saw incontrovertible evidence that terrorists not only could access such information readily but they could use it to dramatic effect that could have strategic consequences. In late 2008, ten terrorists conducted a rampage and hostage siege in the Indian city of Mumbai. The attack was noteworthy for its speed, complexity, high degree of execution, and lethality. Within the first night 10 terrorists had killed almost 200 people and injured more than 350 more. The ten individuals used both the Internet and Google Earth to plan for and carry out their attack.<sup>10</sup> Investigators discovered that the terrorists carried detailed compact discs (CDs) containing high-resolution imagery for geospatial location, target orientation, as well as ingress and egress routing.<sup>11</sup> Terrorists access to information including imagery that was once available only to highly specialized military organizations and heads of state.

Terrorists and insurgents have access to other information that was once the purview of specialists. Such information includes weapons and training that used to require instructors, facilities such as camps, and travel to and from such locations. Today would-be terrorists can readily find instructions on how to synthesize explosives out of chemicals purchased in a pharmacy as well as designs for and instructions on how to build bombs. The four cell members of the so-called “7/7 attack” in London in 2005 allegedly obtained most, if not all of the information they

---

<sup>9</sup> Hearn.

<sup>10</sup> For a summary of the attack, as well as the use of different technologies to facilitate it, see New York Police Department Intelligence Division, “Mumbai Attack Analysis,” New York Police Department, <http://publicintelligence.net/nypd-law-enforcement...mumbai-attack-analysis>.

<sup>11</sup> Anthony L. Kimery, “Mumbai Terrorists’ Use of Google Earth Re-Ignites Concerns,” *Homeland Security Today*, 5 December 2008.

required to develop their bombs from open sources.<sup>12</sup> In addition to helpful advice on how to manufacture explosives, nascent terrorists and insurgents do not need to leave the comfort of their home or Internet café to attend virtual training camps online.<sup>13</sup>

Two decades ago, those plotting resistance against states dreamed of the idea of a “leaderless resistance.” The idea, propagated most famously by Texas White supremacist Louis Beam, posited that action was possible without the need to invest time and resources in an organization for violence.<sup>14</sup> In this way, states seeking to combat sedition would confronted by “...an idea, a thing invulnerable, intangible, without front or back, drifting about like a gas...[that] offered nothing material to the killing.”<sup>15</sup> Today technology allows terrorists to realize the dream of leaderless resistance. Violent extremist terrorists, for example, have changed their method of operations and thrown away hierarchical organizations in favor of a loosely-connected network of individuals, cells, and groups. The current global violent extremist jihad lacks a firm overarching strategy but still has an agenda set by guidelines propagated on the Internet.<sup>16</sup> As jihadi strategist Abu Mus’ab al-Suri wrote in his “Global Islamic Resistance Call,” there is a global system of violence in place rather than a secret organization.<sup>17</sup> In fact this system of violence is what Spanish investigators found in when investigating the Madrid train bombings, al Qaeda did not direct or

---

<sup>12</sup> House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005* (London: The Stationary Office, 2006), 23.

<sup>13</sup> Marco Gercke and Daniel Thelesklaf, “Terrorist Use of the Internet and Legal Response,” *Freedom From Fear Magazine*, Issue 7, <http://www.freedomfromfearmagazine.org/index.php/view=article&catid=50%3Aissue-7&Itemid=161> (accessed 20 May 2012).

<sup>14</sup> Beam’s essay, in which he attributed the idea to Col. Ulius Louis Amoss in a 1962 essay on the same subject, is readily available online. See Louis Beam, “Leaderless Resistance,” *The Seditonist*, 12 February 1992, available online at <http://www.louisbeam.com/leaderless.htm> (accessed 21 May 2012).

<sup>15</sup> T.E. Lawrence, “Evolution of a Revolt,” *Army Quarterly* 1:1, October 1920, available online at <http://usacac.army.mil/cac2/cgsc/carl/resources/csi/Lawrence/lawrence.asp> (accessed 21 May 2012).

<sup>16</sup> Marc Sageman, *Leaderless Jihad*, (Philadelphia: University of Pennsylvania Press, 2008) 144.

<sup>17</sup> Brynjar Lia, *Architect of Global Jihad*, (New York: Columbia University Press, 2008) 421.

execute the attack but only inspired it.<sup>18</sup> Groups and individuals sympathetic to al Qaeda's cause, no matter where they are, can take action and claim a degree of prestige by affiliation: "They are just al-Qaeda in name, trying to acquire the reputation of al Qaeda by using its name."<sup>19</sup>

More disturbing than a global system of resistance is the very real possibility that violent extremist groups will acquire weapons of mass destruction (WMD) and use them. In 2004, influential American political scientist Graham Allison wrote a book about nuclear terrorism. In this book he described not only the possibility of terrorists obtaining WMD by provided chilling detail on how a terrorist might come across nuclear material and fashion it into a bomb.<sup>20</sup> His depiction is alarmist and perhaps melodramatic but served the purpose of identifying a very real national security vulnerability and offered possible courses of action for preventing this type of attack.<sup>21</sup> Some experts view nuclear weapons as something only advanced states are capable of building and employing. Allison's book, along with several disturbing incidents, suggests this line of reasoning is a fallacy. For example, the cult Aum Shinryko managed to manufacture and use sarin gas for its attack on the Tokyo subway system in 1995. Other terrorist groups have sought to obtain radiological material or manufacture deadly toxins such as ricin or botulinum. Nuclear mushroom clouds are a feature in many al Qaeda videos and the fact that Osama bin Laden sought and received a *fatwa*

---

<sup>18</sup> Lia, 335.

<sup>19</sup> Sageman, 129.

<sup>20</sup> Graham Allison, *Nuclear Terrorism: the Ultimate Preventable Catastrophe*, (New York: Times Books/Henry Holt, 2004) Allison's book traces procurement, construction and employment of a cannon type radiological bomb.

<sup>21</sup> Allison

approving the use of WMD suggests to some that it is only a matter of time before terrorists use such weapons against major cities.<sup>22</sup>

All of these trends and incidents are worrisome of policymakers as they suggest that the rise of the non-state actor is the most prevalent threat to US security. When one considers the potential means available to contemporary non-state actors, such as radiological (so-called “dirty”) bombs or crippling cyber attacks, the threat they pose may also be the most dangerous to the nation. The means plus the willingness to use them, in addition to the fact that many non-state actors may have little that stakes can hold at risk, suggests that such strategic actors may not be deterrable. Even if they were deterrable, states tailoring responses face the challenge posed by their distributed nature and ability of terrorists and others to operate alone or in groups. For these reasons and many others, US Government organizations and agencies have faced many challenges in combating such strategic actors. One challenge that organizations and agencies have tried to overcome are the restrictions to actions related to Title 10 and Title 50 authorities as well as Congressional oversight.

### **Pace of Oversight**

“Dysfunctional” was the word the 9/11 Commission used to describe congressional oversight as both the most important area and the most difficult area in need of change following the most dramatic terrorist attacks in U.S. history.<sup>23</sup> The Commission members argued the current structure was inadequate for the counterterrorist focus of today. Their criticism focused on the need to create leading edge technology and

---

<sup>22</sup> The original text of the fatwa is available online at *Jihadica.com*. “Nasir al-Fahd’s Ruling on WMD,” 5 June 2008, available online at <http://www.jihadica.com/nasir-al-fahds-ruling-on-wmd/> (accessed 21 May 2012).

<sup>23</sup> National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States*. (New York: W. W. Norton & Company, 2004), 419-420.

policy to allow policy-makers and warfighters the freedom of action and decisiveness to be successful.<sup>24</sup>

Since the release of the 9/11 Commission report Congress has not changed its oversight structure. They continue to rely upon the separate intelligence and armed services committees to manage oversight organizationally, along Title 10 and Title 50 authorization lines, rather than functionally. This type of oversight relies on the institutional model of oversight described in Chapter One.

Institutional oversight places a level of trust on both the organization and the committee.<sup>25</sup> This trust is necessary because Congress rotates committee membership. Although this may seem inefficient, the purpose of such rotations reflects deny any one Congressman to garner enough experience to dominate the committee as well as the nature of American governance, in which organizations change leadership at the pace that administrations change. Without personnel well-versed in either intelligence or defense issues, effective oversight becomes very difficult even with the best of intentions on both sides of the Congressional aisle.

On December 16, 2005, the *New York Times* broke a story about an NSA surveillance program which collected intelligence on US citizens.<sup>26</sup> The program, authorized after September 11, 2001 by an Executive Order, allowed the NSA to collect signals intelligence on international calls and emails from individuals inside the US without going through a special court procedure.<sup>27</sup> Understandably many individuals both within and outside of government were outraged at the breach of trust and law and a violation of what they saw as personal

---

<sup>24</sup> National Commission on Terrorist Attacks, 419-420.

<sup>25</sup> Frank J. Smist, Jr., *Congress Oversees the United States Intelligence Community: Second Edition 1947-1994* (Knoxville: The University of Tennessee Press, 1994), 20.

<sup>26</sup> James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, 16 December 2005, A1.

<sup>27</sup> Risen and Lichtblau. The program bypassed the FISA courts in some cases which would normally be required if there had not been an Executive Order.

rights and freedoms enshrined in the U.S. Constitution. They demanded an investigation into this alleged overstep. Then on December 23, 2005, another story ran in the *New York Times* detailing who the NSA briefed on the program before it began.<sup>28</sup> The NSA had notified the Congressional “Gang of Eight” as required by Title 50 and a few members had offered written concerns but they did not stop the program.<sup>29</sup>

Oversight did occur as legislated in this instance but Congressional leaders and the American public were both still disappointed with the results. Some of the “Gang of Eight” members pointed to strongly worded letters of concern to belay feelings of public mistrust but this did little to stop the tide of public outrage and resentment over a violation of civil liberties.<sup>30</sup> This example demonstrates how the system of oversight falls short of complying with Madison’s intent in Federalist 51. The executive sought to expand its power and authorities and the legislative branch went along compliantly in the name of national security. These two often competing branches of government were unable to offset or check one another in this instance.

If the 9/11 Commission is correct and the committee structure and jurisdiction in Congress will be next to impossible to change there are other solutions that policy makers have offered to remedy this problem.<sup>31</sup> One such solution is creating a new Title within the U.S. Code to guarantee functional oversight. The establishment of what some has called “Title 60” bridges the gap between intelligence gathering and military operations. The Title 60 proposal would blend Title 10 and Title

---

<sup>28</sup> Douglas Jehl, “DOMESTIC SURVEILLANCE: CONGRESSIONAL LEADERS; Among Those Told of Program, Few Objected,” *New York Times*, 23 December 2005, A1.

<sup>29</sup> Tara M. Sugiyama and Marisa Perry, “THE NSA DOMESTIC SURVEILLANCE PROGRAM: AN ANALYSIS OF CONGRESSIONAL OVERSIGHT DURING AN ERA OF ONE-PARTY RULE,” *University of Michigan Journal of Law Reform*, Fall 2006, 7.

<sup>30</sup> Jehl.

<sup>31</sup> National Commission on Terrorist Attacks, 419.

50 into coherent framework that includes necessary oversight and internal control measures.<sup>32</sup>

The most vocal advocate for Title 60 reform has been Admiral Dennis Blair. During his confirmation hearing to be the Director of National Intelligence (DNI), Admiral Blair unequivocally stated his support for the idea of establishing Title 60.<sup>33</sup> Admiral Blair argued that such a legislative change would dramatically improve the ability of national security organizations and agencies to combat threats including non-state strategic actors. He wanted to bring all of the intelligence and military capability to bear in the global campaign against terrorists.<sup>34</sup> He experienced firsthand the divide between Title 10 and Title 50 while he was the Associate Director of Central Intelligence for Military Support and wanted to solve this problem that had hamstrung overt, covert, and clandestine operations.<sup>35</sup>

While Title 60 resolves the problem of authorities within the DoD and CIA, improving operational effectiveness, it does not resolve the problem of the overlap of authorities and related oversight problems. Title 60 would give both organizations more authority to conduct operations Congress did not design them to do.<sup>36</sup> Title 60 would also not change the fundamental way Congress performs oversight of the CIA or DoD. Without a change in the oversight a Title 60 just blurs an already fuzzy legal situation.

The 9/11 Commission members also recommended the creation of the Director of National intelligence to meld the disparate intelligence

---

<sup>32</sup> David Ignatius, "Outsourcing Intelligence," *Real Clear Politics*, 17 March 2010.

<sup>33</sup> Senate Select Committee on Intelligence, *Nomination of Dennis C. Blair to be Director of National Intelligence*, 111th Cong., 1st sess., 2009.

<sup>34</sup> Senate Select Committee on Intelligence, *Nomination of Dennis C. Blair to be Director of National Intelligence*, 111th Cong., 1st sess., 2009.

<sup>35</sup> Senate Select Committee on Intelligence, *Nomination of Dennis C. Blair to be Director of National Intelligence*, 111th Cong., 1st sess., 2009.

<sup>36</sup> Aaron Epstein, "Sorting Out Who Owns Covert Action Under Title 10 and Title 50," Consortium Consulting Corporation, <http://consortiumconsultingcorporation.blogspot.com/2012/03/sorting-out-who-owns-covert-action.html> (accessed 19 May 2012).

agencies spread across the government.<sup>37</sup> Their goal was to remove the triple-hat relationship and responsibilities the Director Central Intelligence had at the time.<sup>38</sup> In addition they believed the DNI would be able to focus the entire intelligence community on the threat at hand through the provide all-source analysis and plan intelligence operations for the whole of government.<sup>39</sup>

Since the DNI's inception in 2005 there have already been four confirmed directors.<sup>40</sup> The DNI position has proven fraught with difficulties and seemingly insurmountable challenges. For example, the office of the DNI does not control much of the budget for the intelligence community. In addition, the DNI is notionally in charge of all matters related to intelligence, and yet in terms of command and span of control it is a boss among equals within the greater intelligence community. Even worse, the public hold the DNI responsible and becomes a convenient scapegoat within the intelligence community when something goes awry such as a terrorist plot coming together including the 2010 "underwear bomber."<sup>41</sup> The DNI position has not helped with oversight of any of the intelligence agencies because the Director is equal organizationally in rank and authority to the directors of other agencies. This position is unable to deliver on what the members of the 9/11 Commission hoped for because the oversight mechanism surrounding the job was not changed.

### **Oversight in the Future**

The future of Congressional Oversight of operations and intelligence spanning the Title 10 and Title 50 divide is problematic for a number of reasons. The three most significant reasons are the following:

---

<sup>37</sup> National Commission on Terrorist Attacks, 411.

<sup>38</sup> National Commission on Terrorist Attacks, 409.

<sup>39</sup> National Commission on Terrorist Attacks, 411.

<sup>40</sup> *Wikipedia*, s.v. "Director of National Intelligence," [http://en.wikipedia.org/wiki/Director\\_of\\_National\\_Intelligence](http://en.wikipedia.org/wiki/Director_of_National_Intelligence) (accessed 20 May 2012).

<sup>41</sup> Editorial, *San Angelo Standard Times*, 24 May 2010. <http://www.gosanangelo.com/news/2010/may/24/revolving-door-to-top-spys-job/> (accessed 20 may 2012).

declining budget authority; increased use of interagency solutions; and, Congressional misalignment with the current threat that prevents effective oversight from occurring. Detail follows on each item.

First, the current fiscal crisis is spilling into all areas of the government. According to some media sources the intelligence community alone will face US\$25 billion in budget cuts over the next decade.<sup>42</sup> Given these cuts after a period of prolonged growth, organizations and leaders are looking to trim redundant capabilities. One of the primary concerns when standing up CYBERCOM was not duplicating capability or capacity at NSA to avoid Title 10 budget implications.<sup>43</sup> The unintended consequence of creating CYBERCOM was the amalgamation of two agencies under one leader operating under separate Titles of the U.S. Code. The quest to save money rendered questions of authority and oversight moot. As Chapter Three illuminated there are problems inherent in creating an organization of this type.

Second, the mission to defeat non-state strategic actors is necessary and paramount but oversight is legally mandatory. Defense and intelligence organizations and agencies have created interagency processes to enhance their operational effectiveness, and heighten the likelihood of mission success by exploiting the shades of grey that exist between Title 10 and Title 50. SOCOM, found in detail in Chapter 2, is among the best in terms of the military at conducting sensitive military operations around the globe. Since 2004, when the Unified Command Plan changed to make SOCOM a “supported” command in specific instances, its personnel have worked tirelessly in the global pursuit of

---

<sup>42</sup> John Walcott, “Intelligence Budget Cuts Mean U.S. Will Have More Blind Spots,” *Business Week* online 14 November 2011, <http://www.businessweek.com/news/2011-11-14/intelligence-budget-cuts-mean-u-s-will-have-more-blind-spots.html> (accessed 21 May 2012).

<sup>43</sup> Richard Clarke and Robert Knake, *Cyber War*, (New York: HarperCollins, 2010), 38.

terrorists using a range of overt and clandestine means.<sup>44</sup> In parallel with its increased authorities, SOCOM also received a mandate through the 2004 National Defense Authorization Act requiring either the Secretary of Defense or the President approve its missions.<sup>45</sup> To ensure a degree of oversight over these activities Congress passed legislation requiring SOCOM to produce a quarterly report of all clandestine activities it undertakes.

SOCOM's clandestine quarterly report is an attempt at a degree of transparency and oversight of a gray area within the law. Congress has not codified clandestine activity in the law so there is no specific oversight function for it to perform unlike covert action. The clandestine quarterly is one method to keep Congress fully informed of SOCOM activities but this method is not without problems. For example, members of Congress only receive information about sensitive missions after they occur, sometimes months after the fact (given that the report is quarterly). There is no notification, review, or Congressional approval before SOCOM executes clandestine military operations. This method of oversight works on the basis of mutual trust in both action and disclosure but does not prevent or preempt missteps.

The third and final reason that Congressional oversight over Title 10 and Title 50 activities will remain problematic relates to the threats we face. Despite the death of Osama bin Laden and the disruption of al-Qaeda, the threat from terrorist or non-state strategic actors will remain an enduring and potentially devastating one. Individuals and groups will continue to exploit technologies, and morph and adapt, to conduct violence against the United States by virtue of the fact that the country remains the sole superpower globally that will use force to defend its

---

<sup>44</sup> US Special Operations Command, "History United States Special Operations Command, 6<sup>th</sup> ed. 31 March 2008," US Special Operations Command, <http://www.socom.mil/Documents/history6thedition.pdf>, (accessed 19 March 2012), 16

<sup>45</sup> *National Defense Authorization Act for 2004*, Public Law 108-136, 108th Cong., 1st sess. (24 November 2003), §904.

interests. Congressional oversight is misaligned to understand the overt, covert, and clandestine operations used to combat such threats despite the fact the U.S. has been fighting them for more than a decade.

Congress organized its mechanisms for oversight that reflects organizational, departmental stovepipes consistent with the way they wrote the Title 10 and Title 50 legislation in 1947 to deal with the threat posed by the Soviet Union. The character of the current and future threat posed by strategic non-state actors does not fit neatly into either one of these legislative categories for authorization and oversight.

Terrorists by definition seek to exploit such loopholes and weaknesses. If the threat posed by strategic non-states actors is sufficient to warrant change, those charged with combating them have systematically sought expanded authorities while limiting oversight over the actions. The fact is that Congress has not changed legislation or mechanism of oversight to keep pace.

### **Conclusion**

The character of the predominant and potentially most dangerous threat the US faces today and in the future is technologically empowered individuals and groups able to network together and exploit readily available information. The threat posed by such individuals and groups is amorphous in nature and it relies on a leaderless resistance. Such resistance is difficult for our state based defense and intelligence organizations and agencies to comprehend and keep pace with changes to defeat it. Operators often see Title 10 and Title 50 as legislative barriers to more effective operations against such threats. And yet, both Titles draw intelligent lines between organizations allowing government to function properly without excessive overlap or unnecessary oversight over each. Congress organized itself based on departmental lines but the threat has changed making this the least effective way to protect the US. Congress can and must adapt legislation, authorities, and oversight to

ensure its ability to act as a counterbalance against any one branch of government becoming a power unto itself without any transparency or restrictions into its activities.



## CONCLUSION

*Finally, I am concerned that Title 10 operations, though practically identical to Title 50 operations, may not be subjected to the same oversight as covert actions, which must be briefed to the Intelligence Committees.*

Mr. Leon Panetta, QFRs for his CIA appointment

Much time and energy has been devoted to identifying, explaining, and providing recommendations to fix the problems associated with Title 10 and Title 50. Some authors on the subject advocate for changing authorities, changing organizational responsibilities, or even changing the Titles themselves. The investigation in this thesis suggests the Titles themselves work correctly as intended. What can and must evolve, however, is the oversight of actions authorized under Title 10 and Title 50. Congressional oversight is often maligned, and more commonly misunderstood, but it is necessary to the functioning of US democracy and government by preventing any single branch from overstepping its authority.

Contemporary oversight really began in the wake of the Church Committee's investigation into the CIA's alleged covert action oversteps. This landmark legislative Committee, which still exerts an influence on covert action to this day, was the impetus for forming the Senate Select Committee on Intelligence which preceded its House cousin. The intelligence committee oversees agencies governed by Title 50, such as the CIA and NSA, while the armed services committee performs the same function for military agencies authorized under Title 10 such as SOCOM and CYBERCOM.

Historically one can think of the degree of Congressional oversight level as a pendulum. The pendulum swing towards greater oversight

after perceived or real agency oversteps. Examples include the attempted American hostage rescue in Iran (1980), the Iran-Contra Affair (1985-1987), and the Domestic Surveillance Program (the so-called “Warrantless Wiretapping program”; 2001-present). These events or programs have punctuated calls for greater or more specific oversight into government agencies on both sides of the Title 10 and Title 50 divide. The events or programs have not changed the method of oversight only its degree.

As Chapter 2 made clear, there are relationships within the DoD, and between DoD and the CIA that make oversight along organizational lines challenging. SOCOM and the CIA share one of those relationships. Both the Command and the Agency execute similar paramilitary operations but Congress subjects them to different committee oversight based on who is in command at the time. Command of such operations and activities, as this thesis made clear, is one of the characteristics to determine if they are covert or simply clandestine. For example, during Operation NEPTUNE’S SPEAR (the Osama bin Laden raid), uniformed military members executed a mission under the command of the CIA. This allowed the intelligence committees to have oversight, and act as a means of authorization, as opposed to the armed services committee which is traditionally responsible oversight of clandestine activities by military units.<sup>1</sup>

Chapter 3 demonstrated how CYBERCOM and the NSA work together but also how they straddle the Title 10/50 divide differently than SOCOM and the CIA. Both organizations share a single commander or director under a policy known as dual-hatting.<sup>2</sup> This commander or director reports to both the armed services and intelligence committees based on which organization Congress calls him to testify. The implications of this split oversight are clear: subordinates

---

<sup>1</sup> Eric Schmitt and Thom Shanker, *Counterstrike*, (New York: Time Books, 2011), 2.

<sup>2</sup> Richard Clarke and Robert Knake, *Cyber War*, (New York: HarperCollins, 2010), 38.

could conduct potentially illegal activities without a commander knowing, but more troublesome for a democracy is that the potential exists for the director or commander to willingly or unwillingly mislead or misrepresent the activities of two very powerful agencies, in the name of national security, to one or both of the separate Congressional committees charged with their oversight.

The problem suggested by both Chapters 2 and 3 is not with Title 10 and 50 authorities per se, but rather the way in which Congress conducts oversight over them both. The Titles legislatively manage to keep organizations and agencies in their lanes, while at the same preventing excessive government interference in operations and activities. As Chapter 4 suggests, however, the evolving nature of the predominant threat exacerbates and exploits the fissures and loopholes in the current oversight system provided by the different committees. The different departments and agencies charged with combating increasingly capable strategic non-state actors continue to look for more efficient ways to keep pace with and defeat the threat. In doing so these departments and agencies have pushed the boundaries of legislative authorities and further obscured the overlaps that make the differences between Title 10 and 50 difficult to understand by the layman. Whereas U.S. departments and agencies have been proactive and responsive to deal with the evolving nature, Congress has not changed its methods for oversight. Instead Congress remains fully entrenched in outdated modes of behavior, primarily by providing organizational instead of functional oversight.

### So What?

Congressional oversight is about maintaining accountability for and responsibility over extraordinary powers. As Woodrow Wilson noted in 1885, “Quite as important as legislation is vigilant oversight of the administration.”<sup>3</sup> Some authors have made Title 10 and Title 50 the sacrificial lamb for all problems of oversight between the military and intelligence community. Putting the blame on the Titles is a red herring as this thesis has demonstrated.

On the eve of the passage of the landmark Goldwater-Nichols Reorganization Act, MacKubin Thomas Owens offered some advice and counsel to policymakers in an article in *International Security* in 1986.<sup>4</sup> Owens said blamed military failures during the Cold War not the ambiguity inherent in Title 10/50 but rather that leaders would continue to blame these sections of U.S. Code as the source of failure for years to come.<sup>5</sup> Instead he advocated clarifying “the Congressional purpose regarding organizational objectives and fundamental relationships” as part of a different kind of DoD reform.<sup>6</sup>

The kind and scale of reform advocated by Owens though is very difficult. As the 9/11 Commission noted, “strengthening congressional oversight may be among the most difficult and important” of its 42 recommendations.<sup>7</sup> As an indication of the difficulty in reforming oversight, between 1947 and 1975 Congress introduced over 200 bills to increase supervision of the intelligence community but only one passed.<sup>8</sup> Given the challenges identified in Chapter 4 this trend cannot continue.

---

<sup>3</sup> Woodrow Wilson, *Congressional Government* (Boston: Houghton Mifflin, 1885) 297.

<sup>4</sup> MacKubin Thomas Owens, “The Hollow Promise of JCS Reform,” *International Security* 10 no. 3, Winter 1985-1986, 98-111.

<sup>5</sup> Owens, 109.

<sup>6</sup> Owens, 109.

<sup>7</sup> National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States*. (New York: W. W. Norton & Company, 2004), 419.

<sup>8</sup> Harry Howe Ransom, “Congress and the Intelligence Agencies,” *Proceedings of the Academy of Political Science* 32 no 1, 1975, 162

Reversing the current trend will be challenging for a number of reasons. “Under the terms of existing rules and resolutions the House and Senate intelligence committees lack the power, influence, and sustained capability to meet” the challenge of the current security environment.<sup>9</sup>

### **Recommendation**

Currently the system of oversight in both the House and Senate suffers from three problems: jurisdictional complexity, access to information, and partisanship.<sup>10</sup> Each of these alone is a significant problem but when combined together they make effective oversight impossible. Solutions to this problem must contain answers to all three.

Most of this thesis has focused on the jurisdictional and legislative complexity surrounding the Title 10/50 debate. Congress organized the oversight committees along agency lines attempting to keep military functions under the armed services committee and intelligence community members under the intelligence committees. This makes sense from a distance, but the complex threat environment characterized by non-state actors witnessed today challenges this arrangement. This challenge, combined with ambiguous terminology, means that the lines between jurisdiction and oversight become very blurry.

Within the intelligence community it is a truism that information is power. Within the U.S. government system the executive branch holds all of the information regarding clandestine activities. Title 50 requires that the intelligence committees be “fully and completely informed” by the executive branch.<sup>11</sup> Those within the executive branch, however, often interpret this directive much differently than the Congress. Using their legislated exceptions such as “extraordinary circumstances” the executive branch can notify fewer members than the entire committee to

---

<sup>9</sup> National Commission on Terrorist Attacks, 419.

<sup>10</sup> Jennifer Kibbe, “Congressional Oversight of Intelligence: Is the Solution Part of the Problem?” *Intelligence and National Security* 25, no. 1 February 2010, 29-42.

<sup>11</sup> 50 U.S.C.

discussing operations with as few members as “the Gang of Eight” discussed in Chapter One.<sup>12</sup> When operating under this exception only the committee chairs are the ones notified; their staff and other committee members are uninformed. This unequal dialogue hampers the committee’s ability to maintain effective oversight.

The last barrier to effective oversight is partisanship. This obstacle is perhaps the significant one given that partisan politics, conflict, and rancor have risen to new heights within Congress.<sup>13</sup> However Congress can overcome this partisanship with careful rules, making both the armed services and intelligence committee primarily about oversight while limiting budget discussions, the source of disagreement and brinksmanship, to authorizations only.

The 9/11 Commission recommended two solutions to the problem of intelligence oversight because its members believe that “tinkering” with the existing structure would be insufficient for the challenges. They advocated either creating a joint committee for intelligence using the defunct Joint Atomic Energy Committee as a model or combining authorization and appropriation within a single committee in the House and Senate.<sup>14</sup> These are potential solutions to the problems associated with oversight but both attempt large-scale changes while only paying lip-service to Congressional inertia that would prevent enactment. Neither one of these solutions address all three problems raised by Kibbe identified in the beginning of this section.

---

<sup>12</sup> 50 U.S.C.

<sup>13</sup> Jennifer Kibbe, an Associate Professor at Franklin and Marshall College, traces the impact of partisanship within the Intelligence Committees in Kibbe, “Congressional Oversight of Intelligence,” 38-42.

<sup>14</sup> National Commission on Terrorist Attacks, 420.

**Table 4: Proposed Select Intelligence Committee Structure**

<b>Majority Party</b>		<b>Minority Party</b>
Chairman		Vice Chairman
3	<b>At Large Members</b>	2
2	<b>Armed Services</b>	2
2	<b>Defense Appropriations</b>	2
1	<b>Judiciary</b>	1
9	<b>Totals</b>	8

*Source: Author's Original Work*

Table 6.1 offers a proposed solution to solve all three problems. This proposed committee structure for oversight of intelligence activities in the House and Senate, along with minor changes to notification rules, has the potential bring about effective oversight of the overlaps of, and source of confusion between Title 10 and Title 50 activities. The proposed intelligence committee structure addresses the three current barriers to oversight while still acknowledging the reality of the partisan nature of Congress.

The most important characteristic of this proposed structure lies in its title, "Select." The intent is to return to the structure and function of the earliest post-Church Committee intelligence committees.<sup>15</sup> "Select" implies that the Congressional leadership should appoint membership in both the House and Senate Committees to encourage a more moderate political viewpoint. The composition of the proposed Select Committee also reflects the reality of the ruling party, through party majority representation, but is not party proportional as is common practice in other committees. This arrangement can help maintain bipartisanship and offers the promise of promoting cooperation. Oversight of this most complex, challenging, and important aspect of American national security should be above party politics and petty interests.

---

<sup>15</sup> Kibbe, 38.

The proposed committee structure recognizes the jurisdictional complexity present in today's intelligence arena by requiring some members to come from other committees. Rather than attempting to legislate another division between Title 10 and 50, or create a new Title to deal with the new threat as discussed in Chapter 4, this proposed Select Committee structure uses manpower to understand the complex jurisdictional lines. Personnel serving on related committees bring expertise to the intelligence committee without detracting from its oversight focus.

To address the access to information small changes to the rules regarding the Gang of Eight must occur. Currently when the executive branch makes Gang of Eight notifications there are a number of restrictions in place. For example, only the eight members of Congress can be present (and not their staffers), the members are banned from note taking preserving operational security but denying Congress or posterity any sort of record of the discussion, and the members are forbidden from discussing the content of the meeting. Title 50 does not codify these rules but both parties have agreed to them as the Gang of Eight procedures have evolved over time.<sup>16</sup> These steps ensure security at the expense of effective oversight and accountability.<sup>17</sup>

Congress and the executive branch should modify the rules surrounding these notifications to allow a legal counsel member and professional staff member from the House and Senate to attend. This would ensure adequate continuity with the program and offer a way for the Congressmen to ask questions later if they come up. The executive branch should not consider legal counsel and professional staff members

---

<sup>16</sup> Kibbe, 35.

<sup>17</sup> The author searched for instances of Congress leaking classified material from a "Gang of Eight" briefing but was unable to find any. The lack of evidence does not suggest it has never happened but rather that this process, and the individuals within it, have a degree of trustworthiness.

security risks because, unlike members of Congress, they possess security clearances.

Finally much as Executive Order 12333, the well-publicized proscription or ban on assassination, requires dissenting opinions on covert action findings, Congress should document their dissent and attendance at briefings. Currently members receive the briefings of intelligence activities but do not have an avenue of dissent or even a way to mark their attendance at the briefing. By allowing them to document their opinion it provides a conduit back to the executive branch about the collective legislature's state of mind and opinion on intelligence activities. This does not prevent the executive branch from conducting the operation but does provide written record of their position at the time and could potentially influence execution decisions.

The committee structure and rules changes described in the preceding pages do not represent a monumental shift from the current structure; rather, it is a modest first step on a path forward to overcome the three most significant problems related to effective oversight of covert and clandestine operation. While this represents one solution it is not the only one. The most important consideration is that our oversight mechanisms be corrected before the public and some members of Congress read a front-page story like Seymour Hersh's that not only erodes American confidence in its institutions but also causes the pendulum of oversight to severely restrict covert and clandestine operations in response.

## **ACRONYMS**

### ACRONYM – Definition

AUMF – Authorization for the Use of Military Force

CIA – Central Intelligence Agency

COCOM – Combatant Command

CYBERCOM – Cyber Command

DNI – Director of National Intelligence

DoD – Department of Defense

EO – Executive Order

LOAC – Law of Armed Conflict

NSA – National Security Agency

NSC – National Security Council

OSS – Office of Strategic Services

SAASS – School of Advanced Air and Space Studies

SOCOM – Special Operations Command

SOF – Special Operations Forces

SROE – Standing Rules of Engagement

STRATCOM – Strategic Command

TMA – Traditional Military Activity

US – United States

USAF – United States Air Force

USC – United States Code

WMD – Weapons of Mass Destruction

## BIBLIOGRAPHY

- Allison, Graham. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. New York: Times Books/Henry Holt, 2004.
- Ambinder, Marc and D.B. Grady. *The Command: Deep Inside the President's Secret Army*. John Wiley & Sons, 2012. Kindle e-book.
- Andrues, Wesley R. "What U.S. Cyber Command Must Do." *Joint Forces Quarterly* 59 (4th Quarter 2010): 115-120.
- "Anonymous Gain Access to FBI and Scotland Yard Hacking Call." *BBC News*, 3 February 2012. <http://www.bbc.co.uk/news/world-us-canada-16875921?print=true>
- Bamford, James. *Body of Secrets*. New York: Anchor Books, 2002.
- Bernsten, Gary. *Human Intelligence, Counterterrorism, & National Leadership*. Washington, DC: Potomac Books, 2008.
- Beam, Louis. "Leaderless Resistance." *The Seditonist*, 12 February 1992.
- Born, Hans and Loch K. Johnson. "Balancing Operational Efficiency and Democratic Legitimacy." In *Who's Watching the Spies?* Edited by Hans Born, Loch K. Johnson, and Ian Leigh, 225-240. Washington: Potomac Books, 2005.
- Bowden, Mark. *Worm*. New York: Atlantic Monthly Press, 2011.
- Bronk, Chris. "Treasure Trove or Trouble: Cyber-Enabled Intelligence and International Politics." *American Intelligence Journal* 28, no. 2 (2010): 26-30.
- Bumiller, Elisabeth. "Army Broadens Inquiry into Wikileaks Disclosure." *The New York Times*, 30 July 2010.
- Caparini, Marina. "Controlling and Overseeing Intelligence Services in Democratic States." In *Democratic Control of Intelligence Services*, edited by Hans Born and Marina Caparini, 3-24. Burlington: Ashgate, 2007.
- Clarke, Richard and Robert Knake. *Cyber War*. New York: HarperCollins, 2010.

Colby, William and Peter Forbath. *Honorable Men: My Life in the CIA*. (New York: Simon and Schuster, 1978.

“Congress to Restrict Use of Special Ops.” *The Washington Times*, 13 August 2003.  
<http://www.washingtontimes.com/news/2003/aug/13/20030813-120409-8659r/?page=all>.

Cumming, Alfred. *Sensitive Covert Action Notifications: Oversight Options for Congress*. CRS Report for Congress. Washington: Congressional Research Service, 25 September 2009.

Daugherty, William J. *Executive Secrets: Covert Action and the Presidency*. Lexington: The University Press of Kentucky, 2004.

Dobbs, Michael. *Saboteurs: The Nazi Raid on America*. New York: Random House, 2004.

Dozier, Kimberly. “Officers: No Plans for CIA to Run War.” *Philadelphia Inquirer*, 8 March 2012.

Emerson, Steven. *Secret Warriors: Inside the Covert Military Operations of the Reagan Era*. New York: G.P. Putnam’s Sons, 1988.

Epstein, Aaron. “Sorting Out Who Owns Covert Action Under Title 10 and Title 50.” Consortium Consulting Corporation.  
<http://consortiumconsultingcorporation.blogspot.com/2012/03/sorting-out-who-owns-covert-action.html> (accessed 19 May 2012).

Executive Order 11828. Establishing a Commission on CIA Activities Within the United States, 4 January 1975.

Executive Order 11905. United States Foreign Intelligence Activities, 19 May 1976.

Executive Order 12333. United States Intelligence Activities, 4 December 1981.

Federation of American Scientists. “CJCS Instruction 3121.01A, 15 January 2000,” [http://fas.org/man/dod-101/dod/docs/cjcs\\_sroe.pdf](http://fas.org/man/dod-101/dod/docs/cjcs_sroe.pdf).

Fenno, Richard F., Jr. *Congressmen in Committees*. Boston: Little, Brown and Company, 1973.

Ferrell, William H., III. "No Shirt, No Shoes, No Status: Uniforms, Distinction, and Special Operations in International Armed Conflict," *Military Law Review* 178, (Uniforms, Distinctions, and Status, 2003): 94-140.

Garamone, Jim. "Questions Abound in Cyber Theater of Operations, Vice Chairman Says." *Armed Forces Information Service*, 9 June 2009.

Gercke, Marco and Daniel Thelesklaf. "Terrorist Use of the Internet and Legal Response." *Freedom From Fear Magazine*, Issue 7.  
<http://www.freedomfromfearmagazine.org/index.php/view=article&catid=50%3Aissue-7&Itemid=161> (accessed 20 May 2012).

Google. "Google Earth Frequently Asked Questions." Google.  
<http://support.google.com/earth/bin/answer.py?hl=en&answer=187961&topic=2376010&ctx=topic> (accessed 20 May 2012).

Graham, Bradley. *By His Own Rules*. New York, PublicAffairs, 2009.

Gross, COL Richard "Different Worlds: Unacknowledged Special Operations and Covert Action" Carlisle Barracks, PA: Army War College, 2009.

Hamilton, Lee H., and Jordan Tama. *A Creative Tension: the Foreign Policy Roles of the President and Congress*. Washington: Woodrow Wilson Center Press, 2002.

Harlow, Bill, and George Tenet. *At the Center of the Storm: My Years at the CIA*. New York: Harper, 2007.

Hearn, Kelly. "Terrorist Use of Google Earth Raises Security Fears." *National Geographic News*, 12 March 2007.  
<http://news.nationalgeographic.com/news/pf/93861668.html>

Hersh, Seymour M. "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years." *New York Times*, 22 December 1974.

Hersh, Seymour M. "The Gray Zone." *The New Yorker*, 24 May 2004.

House of Commons. *Report of the Official Account of the Bombings in London on 7th July 2005*. London: The Stationary Office, 2006.

“House Panel Votes to Build Missile Defense Site on East Coast Despite Pentagon Disapproval,” *The Washington Post*, 9 May 2012.

Ignatius, David. “Outsourcing Intelligence.” *Real Clear Politics*, 17 March 2010.

*Intelligence Authorization Act for 1981*. Public Law 96-450. 96th Cong., 2nd sess., 14 October 1980.

*Intelligence Authorization Act for Fiscal Year 1991*. Public Law 102-88. 102nd Cong., 1st sess., 14 Aug 1991.

International Committee of the Red Cross. “Convention (III) relative to the Treatment of Prisoners of War, 12 August 1949.”  
<http://icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e63bb/6fef854a3517b75ac125641e004a9e68> (accessed on 24 May 2012).

Jehl, Douglas. “DOMESTIC SURVEILLANCE: CONGRESSIONAL LEADERS; Among Those Told of Program, Few Objected.” *New York Times*, 23 December 2005.

Jihadica. “Nasir al-Fahd’s Ruling on WMD.”  
<http://www.jihadica.com/nasir-al-fahds-ruling-on-wmd/> (accessed 21 May 2012)

Joint Pub 3-05.1. *Joint Special Operations Task Force Operations*, 26 April 2007.

Johnson, Loch K. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: The University Press of Kentucky, 1985.

Johnson, Loch K. “Governing in the Absence of Angels.” In *Who’s Watching the Spies?*, edited by Hans Born, Loch K. Johnson, and Ian Leigh, 57-78. Washington: Potomac Books, 2005.

Khong, Yuen Foong. *Analogies at War*. Princeton: Princeton University Press, 1992.

Kibbe, Jennifer D. “The Rise of the Shadow Warriors.” *Foreign Affairs*, March/April 2004, 102-115.

Kibbe, Jennifer D. “Congressional Oversight of Intelligence: Is the Solution Part of the Problem?” *Intelligence and National Security* 25, no. 1, February 2010: 24-49.

Kimery, Anthony L. "Mumbai Terrorists' Use of Google Earth Re-Ignites Concerns." *Homeland Security Today*, 5 December 2008.

Lamb, Christopher and Evan Munsing. *Secret Weapon: High-Value Target Teams as an Organizational Innovation*. Washington, DC: NDU Press, 2011.

Lawrence, T.E. "Evolution of a Revolt." *Army Quarterly* 1, October 1920.

Lia, Brynjar. *Architect of Global Jihad*. New York: Columbia University Press, 2008.

Lotz, George B., II. "The United States Department of Defense Intelligence Oversight Programme: Balancing National Security and Constitutional Rights." In *Democratic Control of Intelligence Services* edited by Hans Born and Marina Caparini, 109-124. Burlington: Ashgate, 2007.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 2nd ed. Washington: CQ Press, 2003.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 4th ed. Washington: CQ Press, 2009.

Lynn, William J, III, US Deputy Secretary of Defense. Defense Information Technology Acquisition Summit, Washington DC, 12 November 2009.

Madison, James. "The Federalist Number 51." *Independent Journal*, 6 February 1788.

McAndrew, Michael. "Wrangling in the Shadows: The Use of United States Special Forces in Covert Military Operations in the War on Terror." *Boston College International and Comparative Law Review* 29, no. 1 (1 December 2006): 152-164.

McCormick, Charles H. *Hopeless Cases: The Hunt for the Red Scare Terrorist Bombers*. Lanham: University Press of America, 2005.

Nakashima, Ellen. "When Is a Cyberattack a Matter of Defense?" *The Washington Post*, 27 February 2012.

Nakashima, Ellen. "NSA Thwarted in Cybersecurity Initiative." *The Washington Post*, 28 February 2012.

Nakashima, Ellen. "Military Leaders Seek Higher Profile For Pentagon's Cyber Command Unit." *The Washington Post*, 1 May 2012.

National Commission on Terrorist Attacks. *The 9/11 Commission Report: Final Report of the National Commission On Terrorist Attacks Upon the United States*. New York: W. W. Norton & Company, 2004.

National Security Agency/Central Security Service. "NSA/CSS Frequently Asked Questions."  
[http://www.nsa.gov/about/faqs/about\\_nsa.shtml](http://www.nsa.gov/about/faqs/about_nsa.shtml) (accessed 21 April 2012).

New York Police Department Intelligence Division. "Mumbai Attack Analysis." New York Police Department.  
<http://publicintelligence.net/nypd-law-enforcement...mumbai-attack-analysis>.

Owens, MacKubin Thomas. "The Hollow Promise of JCS Reform."  
*International Security* 10, no. 3, Winter 1985-1986: 98-111.

Parks, W. Hays. "Special Forces' Wear of Non-Standard Uniforms."  
*Chicago Journal of International Law* 4, no. 2 (Fall 2003): 493-560.

Pellerin, Cheryl. "Cyber Operations Give Leaders New Options, Official Says." *American Forces Press Service*, 12 April 2012.

Pillar, Paul R. "Unintelligent Design." *The National Interest* 109 (Sep/Oct 2010): 43-50.

Priest, Dana and William Arkin. *Top Secret America*. New York: Little, Brown and Company, 2011.

Public Law 80-253. *National Security Act of 1947*, sec 501, 80th Cong., 1st sess.

Public Law 93-559. *Foreign Assistance Act of 1961*, sec. 662, 93rd Cong., 2nd sess.

Public Law 107-40. *Authorization to Use Military Force*, 107th Cong., 1st sess.

Public Law 108-136. *National Defense Authorization Act for 2004*, sec 904, 108th Cong., 1st sess.

Ransom, Harry Howe. "Congress and the Intelligence Agencies."  
*Proceedings of the Academy of Political Science* 32, no 1, 1975.

- Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." *New York Times*, 16 December 2005.
- Rosenbach, Eric and Aki J. Peritz. *Trials by Fire, Counterterrorism and the Law*. Cambridge: Belfer Center for Science and International Affairs, 2010.
- Rumsfeld, Donald. *Known and Unknown*. New York: The Penguin Group, 2011.
- Saad, Lydia. "Congress Ranks Last in Confidence in Institutions." Gallup Politics. <http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx> (accessed 19 March 2012).
- Sageman, Marc. *Leaderless Jihad*. Philadelphia: University of Pennsylvania Press, 2008.
- Secretary of Defense and Secretary of Homeland Security. Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity, 27 September 2010.
- Schmitt, Eric and Thom Shanker. *Counterstrike*. New York: Times Books, 2011.
- Shultz, Richard H., Jr. "Showstoppers." *The Weekly Standard* 9, no. 19, 26 January 2004.  
<http://www.weeklystandard.com/Content/Public/Articles/000/000/003/613twavk.asp>.
- Singer, P.W. "Essay: Double-Hatting Around the Law." *Armed Forces Journal*, June 2010.  
<http://www.armedforcesjournal.com/2010/06/4605658/>.
- Smist, Frank J., Jr. *Congress Oversees the United States Intelligence Community: Second Edition 1947-1994*. Knoxville: The University of Tennessee Press, 1994.
- Stone, COL Kathryn "'All Necessary Means'—Employing CIA Operatives in a Warfighting Role Alongside Special Operations Forces" Carlisle Barracks, PA: Army War College, 2003.
- Sugiyama, Tara M. and Marissa Perry. "THE NSA DOMESTIC SURVEILLANCE PROGRAM: AN ANALYSIS OF CONGRESSIONAL OVERSIGHT DURING AN ERA OF ONE-PARTY RULE." *University of Michigan Journal of Law Reform*, Fall 2006.

- US House. *House Select Committee on Intelligence*. 94th Cong., 1st sess., H. R. 138, 19 February 1975.
- US House. *Joint Explanatory Statement of the Committee of Conference*. 102nd Cong., 1st sess., 1991, HR 1455.
- US House. *National Defense Authorization Act for Fiscal Year 2012*. 112th Cong., 1st sess., 2011, HR 112-329-Part 1.
- US House. *Proposed Fiscal 2013 Defense Authorization as it Relates to Information Technology and Cyber Operations*, 112th Cong., 2nd sess., 2012.
- US Senate. *Congressional Record*. 94<sup>th</sup> Cong., 1<sup>st</sup> sess., 21 January 1975.
- US Senate. *Select Committee to Study Governmental Operations with Respect to Intelligence Activities*. 94th Cong., 1st sess., S. R. 21, 27 January 1975.
- US Senate. *Legislative Proposals to Strengthen Congressional Oversight to the Nation's Intelligence Agencies: Hearings before the Subcommittee on Intergovernmental Relations*, 93rd Cong., 2<sup>nd</sup> sess., 1974.
- US Senate, *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94th Cong., 2nd sess., S.R. 400, 19 May 1976.
- US Senate, *Authorizing Appropriations for Fiscal Year 1991 For the Intelligence Activities of the U.S. Government, the Intelligence Community Staff, the Central Intelligence Agency Retirement and Disability System and for Other Purposes*, 102nd Cong., 1st sess., SR 102-85, 19 June 1991.
- US Senate. *Nomination of Dennis C. Blair to be Director of National Intelligence*. 111th Cong., 1st sess., 2009.
- US Special Operations Command. "History United States Special Operations Command, 6<sup>th</sup> ed. 31 March 2008." US Special Operations Command.  
<http://www.socom.mil/Documents/history6thedition.pdf>  
(accessed 19 March 2012).
- US Strategic Command. "CYBERCOM Fact Sheet."  
<http://www.stratcom.mil/factsheets/Cyber-Command> (accessed 3 May 2012).

- Walcott, John. "Intelligence Budget Cuts Mean U.S. Will Have More Blind Spots." *Business Week* online, 14 November 2011.  
<http://www.businessweek.com/news/2011-11-14/intelligence-budget-cuts-mean-u-s-will-have-more-blind-spots.html> (accessed 21 May 2012).
- Walker, Paul. "Traditional Military Activities in Cyberspace: Preparing for 'Netwar.'" *Selected Works*.  
[http://works.bepress.com/paul\\_walker/2](http://works.bepress.com/paul_walker/2) (accessed 23 May 2012).
- Waterman, Shaun. "Cyber Warfare Rules Still Being Written." *The Washington Times*, 20 March 2012.
- Whitcover, Jules. *Sabotage at Black Tom: Imperial Germany's Secret War in America, 1914-1917*. Chapel Hill: Algonquin Books, 1989.
- Wilson, Woodrow. *Congressional Government*. Boston: Houghton Mifflin, 1885.

